 DOI: https://doi.org/10.12345/daglyqyfzyj.v2i7.19610

Discussion on the Security Management of the Archive Database under the Network Environment

Aijun Guo

Cangzhou City Labor Ability Appraisal Center, Cangzhou, Hebei, 061001, China

Abstract

Driven by the rapid development of information technology, various parts of the world have invested in the construction of digital archives, which has opened up a new era of network for archive management, achieving efficient aggregation, systematic organization, and convenient utilization of archive resources. However, the various threats faced by archival databases in the network field are increasingly severe, and how to effectively improve the security of archival databases has become an important issue that needs to be urgently addressed. The paper is based on the current situation of archive database construction, deeply analyzes the key factors that have a significant impact on archive database security, and proposes corresponding security management strategies on this basis, in order to comprehensively improve the security protection level of archive databases.

Keywords

network environment; archive database; security management

浅议网络环境下的档案数据库安全管理

郭爱军

沧州市劳动能力鉴定中心，中国·河北 沧州 061001

摘　要

在信息科技迅猛发展的推动下，世界各地纷纷投入到数字档案馆建设的热潮之中，这为档案管理事业开启了全新的网络时代，实现了档案资源的高效聚合、系统化整理及便捷利用。然而，网络领域中的档案数据库所面临的各类威胁日益加剧，如何有效提升档案数据库的安全性已成为亟待解决的重要课题。论文立足于当前档案数据库建设的实际情况，深度剖析对档案数据库安全产生重大影响的关键因素，并在此基础上提出相应的安全管理策略，以期全面提高档案数据库的安全防护水平。

关键词

网络环境；档案数据库；安全管理

1 引言

在数字化社会背景下，档案管理已逐渐转变为网络信息化。这种趋势虽方便实现数据高效共享，却亦伴随数据处理风险。若无适当管理策略，网络环境下的数据安全性势必受到威胁，进而干扰档案数据库正常运用。网络环境下档案数据库易遭受数据泄漏、恶意删减及无故篡改等问题困扰，严重影响档案数据利用与稳定性。当下不少档案数据库安全管理员信息安全意识淡薄，操作行为欠规范，制度建设尚待完善，以致档案数据库安全管理能力难以提高。因此，有必要对档案数据库的信息管理进行更严格的安全保护。

2 网络环境对档案数据库安全管理的挑战

2.1 警惕安全意识淡薄

传统档案数据库仅授权给特定使用者，但如今网络环境扩大了其公开范围，增加了档案信息安全风险，从而增大了信息泄露可能性。目前，档案数据库安全管理工作在资源配置方面尚待进一步完善，同时，对于数字档案工作项目的使用分级也未能够根据不同用户之间的差异进行详尽梳理与区分。这两项问题都有可能在今后的内部管理中引发潜在的风险和漏洞。若档案管理体系规划及管理不当，所有档案内容将暴露于同一层面，引发档案管理混乱并增加信息安全风险。依据目前数据库管理的实际状况来看，无论是用户群体抑或是系统管理者，在档案安全性方面都表现出了明显的疏忽与不足，此问题直接引发了档案数据管理的混乱现象[1]。

2.2 数字化档案安全管理从业者素质亟待提升

鉴于传统档案信管模式，管理者只需处理纸质文件，而数字化环境则需先将其转为电子形式，然后进行存储与管理。因此，档案管理员需具备基础电脑操作技能，掌握线上档案信息处理方法。然而，目前档案管理团队尚存在部分专业素质不高者，整体水平有待提高，特别是在计算机应用方面表现欠佳，可能无法熟练运用数字化技术或掌握相关

【作者简介】郭爱军（1974–），男，中国河北东光人，助理馆员，从事业务档案或档案管理研究。

知识，从而对数字化档案安全管理产生直接或间接的负面影响。

2.3 无完备之数字档案安全管理法制

据当前部分公立机构档案管理状况来观察，诸多单位于档案安全管理制度层面未能遵法守法。在实际情况中，中国并未制定统一的国家级数字档案安全管理相关法规。由于政策的不确定性和模糊性，使得数字档案安全管理制度的运作陷入了无序或无效的状态，局部的档案管理员无法明确自身的职责范围，尤其是在处理涉及多个部门的档案管理事务时，各部门之间的管理要求和规定存在着显著的差异。因此，如何加强各部门之间的沟通协调，提高协同工作的效率，从而建立起全面而有效的安全防护体系，这无疑是当前数字档案安全管理制度所面临的迫切需要解决的问题。如果没有一套完善的安全管理制度作为保障，那么就有可能出现档案使用记录和录入信息不完整、管理混乱以及管理员随意操作等诸多问题，这些都将对档案管理的质量产生严重的负面影响，同时也会削弱档案数据的安全性。

2.4 无数字档案信息安全评估标准

随着互联网技术的发展，档案信息安全管理所面临的信息曝光风险也日益加剧，加剧信息安全重要性；同时，黑客行为易导致档案信息泄露，甚至危及其他关键数据安全。实践中，不少机构并未完全依照相关规定来处理档案信息，例如遗漏存储或上传操作会对资料构成损害。同时，绝大部分档案信息尚无完善的安全评估体系，缺少权威的安全性评估标准。随着电子技术推动社会变革，电子信息扫描和接收频繁，档案管理面临的安全问题愈发显现。由于任何流程疏忽都有可能引发档案信息丢失或泄露等严重风险，影响到档案数据安全性并减弱其保护效力。

3 档案数据库安全风险影响因素解析

3.1 人为因素

档案数据库安全管理涵盖多种角色，如第三方服务企业、内部员工及外来访客等。特别是第三方服务机构，身为档案数据库信息化建设的主要服务提供商，承担了档案信息的编辑与管理职能。其重要性不言而喻，一旦档案信息源发生泄漏，将对整体安全性产生重大影响。值得注意的是，第三方服务商需要直接接触档案原始信息并涉及大量的电子设备和产品，因此如果该环节安全措施不足，将加大情报泄露的可能性。内部员工身为直接应用档案信息的专家，拥有直接修订档案原始数据的权限。然而，当前档案安全管理措施多以抵御外来威胁为主导，却未充分考虑内部人员作案带来的潜在破坏。如若规章制度存在漏洞，无论是内部员工无意或故意的行为，均可能对档案信息安全构成隐患。而来自外部人员的风险则主要体现在误操作与黑客恶意攻击等方面 [2]。

3.2 环境要素

尽管网络化数据库管理系统降低了纸质损耗风险，但仍需遵守物理存储规则。例如，环境污染和自然灾害可能破坏存储设施，因此数据信息储藏空间需采用抗磁性、耐火性的电子设备进行防护。建立常规维护制度和实时监测电子库房环境对保障数据库运行至关重要。软硬件设备是数据库正常运转的基础，如果在性能运用和系统维护中出现疏漏，会影响数据库安全。目前，数据库架构主要有 B/S 和 C/S 两种形式，它们在网络接入点上存在差异。中国档案管理体系中 C/S 模式有一定优势，但在数字档案服务展示和应对网络安全威胁方面仍需提高。

4 强化档案数据库安全管控策略的建议

4.1 深化了解，提高决策能力，明确权责界限

档案管理者必须深入理解档案管理信息化的紧迫性以及其所具有的重要意义，彻底颠覆陈旧的观念，始终保持严谨的态度来优化并拓宽档案管理的领域。也应高度重视档案管理所发挥出的引导效用，努力持续提升档案系统的信息科技程度；明晰各部门的职责分工，携手推进档案管理系统的全方位升级以及信息化技术的蓬勃发展。

4.2 深化档案数据库安全机制体系构建

对于保障档案数据安全管理至关重要的制度建设，其地位是不容忽视的基石。我们应当订立一套全面系统的安全制度，这其中包括了安全等级划分、数据保密措施、数据备份策略以及档案数据库的监督和应急处理等关键环节。这些措施将致力于确保档案数据库的安全性得到坚实可靠的保证。为了实现这个目标，我们必须制定一份详尽周全的档案数据库安全规划，严格遵守《电子文件归档与管理规范》中的相关规定，对档案数据库的顶层架构进行精确的设计，明确各部门的职责权限，以实现协同合作的安全管理模式。此外，我们还需要加强档案数据库的分级分类管理，根据各类档案的价值差异，实施分级分类保护，从而提升档案数据库的针对性安全保障水平。最后，我们要完善覆盖档案数据生命周期全程的安全监控监测机制，以便能够及时地发现并消除潜在的风险，进一步增强档案数据库的整体安全防护能力 [3]。

4.3 提升科技维护档案数据安全性之能力

伴随着信息科技的持续演进与创新，多种新型技术层见叠出。若无深厚的技术实力为依托，档案数据库的安全管控便显得虚无缥缈。将诸如区块链之类的尖端技术引入档案数据库构建，能提升文档数据的安全性和稳定性，维护其真实性和原始性，有效缓解可能出现的风险，彻底消除档案被窃取、丢失或恶意修改的威胁。由此，实际的档案数据库安全性得到了有力保障。传统的加密学与数据追踪技术同样为档案数据安全提供关键支持，同时也不能忽略对其加密和数据追踪的强化执行。

4.4 强化档案管理团队建设

重点关注充实人员储备，吸引更多拥有高超档案管理专业知识和精湛计算机技能的优秀人才的加入。加强档案管

理实操训练，使相关人员更加深入地了解信息化转型的内涵。在此基础上，不断提供丰富的学习和培训机会，以全面改善专业素质，构建专业化的人才梯队，为未来档案信息安全管理提供强大的技术保障，进一步拓展档案信息管理的发展空间。

4.5 强化档案数据库数据采集工作

档案数据采集，这个被誉为是实体档案收集归档的核心环节，也是档案管理工作的基石和首要步骤之一，其安全性无疑会直接影响到档案数据库的稳定性以及应用效率。在进行数据收集的阶段，对数据的格式、来源及其结构进行审慎而严谨的检查和核验，以便为接下来的档案数据库建设铸造一座坚实的根基。只有那些具有相似结构、同源数据以及统一格式的档案数据，才能够真正地成为值得信赖的数据库保管资料。在这一过程中，应积极运用诸如区块链、数据溯源等前沿科技手段，以确保档案数据库的真实性和原始性，提高档案数据库的安全防护能力[4]。

4.6 加强档案数据库数据传输安全性保障措施

当执行档案资料数据的传输任务时，务必要对数据传输的安全性给予极高的关注度，确保档案数据库内部所有的信息都不会有任何泄露的可能性。严格地实行档案数据传输过程中的安全责任制度，签订相关的安全协议，将每个环节安全责任人的工作职责和义务进行明确的规定，以便更有效地防范档案数据在传输过程中所面临的各种潜在风险。

4.7 构建档案数据库存储安全体系

档案数据库作为档案存藏的核心载体，与实体档案库房有着同样的重要性。在实体库房中，严格执行”八防”标准至关重要，即防水、防火、防盗、防潮、防蛀、防鼠以及防尘。强化档案数据库管理系统软硬件装备的更新换代力度，追加充足的经费投入，优化信息基础设施的配置，提升设备应对各种风险的能力，从而从根本上确保数据库的存储安全。充分发挥防火墙的防护作用，有效阻止未获授权者对数据库的非法访问，同时加强对风险点的监测与研究工作，以便能够及时发现潜在问题，持续提升修复漏洞的能力，进而实现对档案数据库存储安全的全方位保护[5]。

4.8 强化档案数据库数据共享的安全管理体系

应信息技术布局的要求，档案数据库的建设目标在于提高档案数据的应用价值，进而推动档案数据共享机制的顺利运行。目前，各层级档案管理机构对档案资源共享给予了高度重视，多个省市已展开成效显著的共享实践，例如，诸多民生档案已实现异地查询等多项服务，大大方便了档案使用者。构建可靠的身份验证与授权系统，严格遵守数据安全规定，科学规划用户访问权限。在严格控制档案数据权限的同时，也应加强档案使用者的权限管理，将二者有机融合。以此确保档案数据在分享过程中的安全性和稳定性。

5 结语

在可预见的未来一段较长时期之内，档案数据库在互联网环境中的建设和配置无疑将成为档案管理领域的重要环节以及关键所在，与此同时，档案数据库的安全监控及其相关措施等方面都需要进行全方位、立体式的革新与突破。因此，我们将不断深化对于网络环境中数据库档案管理方式的深入挖掘和探讨，期望最终能够制订出适用于各个不同行业领域的全面性管理策略及规划，从而有力地推动中国档案事业向健康、有序、繁荣发展，并保持其稳定运行态势。

参考文献

[1] 陈喜华.网络环境下档案数据库安全管理研究[J].兰台内外,2022(18):30-32.

[2] 姜海龙.网络环境下档案管理工作的创新思考[J].办公室业务,2023(23):168-170.

[3] 牛福厚.大数据背景下档案信息化管理的问题与对策研究[J].活力,2023,41(15):145-147.

[4] 袁方,王帅,杭国锋.网络环境下档案管理工作的创新思考[J].网络安全技术与应用,2023(1):99-101.

[5] 张菲.网络环境下数字档案管理应用安全分析[J].黑龙江档案,2022(4):286-288.