工程档案信息化管理的安全风险及防范措施

赵苓艳

神东工程项目管理公司 内蒙古 鄂尔多斯 017000

【摘　要】：随着信息技术的广泛应用，工程档案管理正逐步由传统纸质形态向信息化、数字化和智能化方向转变。这一变革在提高档案利用效率、降低存储成本、提升数据共享水平方面具有显著优势，但同时也带来了诸多安全风险，包括数据泄露、信息篡改、系统瘫痪以及管理责任缺位等。若未能建立科学完善的安全防控机制，不仅可能导致工程资料丢失，还会对项目质量监督、工程责任追溯及行业信用体系产生负面影响。本文系统分析了工程档案信息化管理中存在的主要安全风险，从技术、管理和法律制度等角度提出防范措施，以期为工程建设领域的档案管理提供有价值的参考。

【关键词】：工程档案；信息化管理；安全风险；防范措施；数据保护

DOI:10.12417/2811-0528.25.022.080

引言

工程档案作为记录建设项目全过程的重要载体，涵盖设计、施工、监理、验收等环节的关键资料，是工程质量责任追溯和后期运维管理的重要依据。在信息化浪潮推动下，工程档案管理逐渐摆脱纸质依赖，实现了电子化存储与在线共享。然而，信息化的便利背后隐藏着复杂的安全隐患。黑客入侵、病毒攻击、数据篡改、人为疏忽等问题频频出现，严重威胁档案数据的完整性和真实性。

安全问题不仅仅是技术层面的问题，还涉及管理制度和人员素质。若缺乏统一规范的制度保障与科学有效的防范机制，信息化带来的优势将被风险抵消。因此，研究工程档案信息化管理的安全风险并提出切实可行的防范措施，具有现实紧迫性和战略意义。

1 工程档案信息化管理的现状与特征

1.1 信息化发展趋势

近年来，随着大数据、云计算、人工智能等新一代信息技术的迅猛发展，工程档案管理逐渐从传统的纸质化、分散化模式，向网络化、智能化和共享化方向演进。越来越多的工程建设单位开始建立统一的档案信息管理平台，实现档案资料的网络化存储、在线调阅与远程共享。各参建单位和管理部门可以通过统一账号和权限系统，在同一平台上实现资料的实时上传、调用与更新，大大提高了工程建设过程中信息传递与沟通的效率。同时，智能化的档案检索、分类和自动归档功能，有效减少了人工整理中的错误和疏漏，使档案管理的准确性与便捷性显著提升。随着区块链技术的应用探索，未来档案管理还可能实现更高水平的可追溯性和防篡改性，为工程建设的全生命周期管理提供更加可靠的数据支持。

1.2 现有体系的优势

信息化档案系统的普及，突破了传统纸质档案在时间和地域上的限制，实现了跨部门、跨区域的协同共享。无论是在项目建设阶段，还是在竣工后的运维管理中，相关单位都能通过信息化平台随时随地查阅和调取所需的工程资料，极大提升了工作效率与协同水平。相比传统的纸质档案，电子化存储节省了大量的物理空间成本，同时也便于批量备份与多地存储，提升了资料的安全性和长期保存的可靠性。

此外，信息化档案的可复制性和可追溯性优势，为后期的分析与决策提供了数据基础。例如，在工程项目的维修、改造和扩建过程中，管理者可以快速调取历史数据，分析施工参数和设备资料，为科学决策提供依据。相较于传统纸质档案可能因保存不当而出现的损坏、丢失、难以修复等问题，信息化档案系统能够实现自动备份与定期更新，有效降低了资料丢失的风险。正因如此，信息化档案系统不仅是一种存储和管理手段，更逐渐成为工程建设全过程数字化管理的重要组成部分，为工程质量管控和后期资产管理提供有力保障。

1.3 潜在风险的隐蔽性

尽管信息化档案系统具备显著优势，但其潜在风险往往更具隐蔽性和突发性。一方面，信息化系统依赖于网络与硬件设施，一旦遭遇黑客攻击、病毒入侵或恶意篡改，可能在短时间内造成大范围的数据丢失或泄露，甚至引发严重的经济与信誉损失。另一方面，操作人员的不当操作或管理漏洞，也可能带来意想不到的风险。例如，权限分配不合理可能导致机密资料泄露，缺乏定期备份可能在系统故障时造成无法弥补的损失。由于信息化系统的复杂性，很多问题在早期难以及时被发现，等到出现明显后果时，往往已经波及多个部门和环节，其影响范围和破坏力远超预期。

更值得注意的是，信息化档案系统的风险不仅来自外部攻击，还可能源于内部管理不到位。例如，部分单位过度依赖第三方平台提供存储与安全保障，但缺乏自身的安全防控措施和应急预案，一旦外部服务商出现故障，就可能导致数据链条整体瘫痪。此外，随着信息化程度不断加深，数据量呈指数级增长，如果缺乏完善的数据治理体系，也可能出现数据冗余、版本混乱、信息失真等问题，进而影响档案的权威性和可用性。

因此，虽然信息化档案管理在效率与安全性上具有明显优势，但其风险防控必须同步跟进。除了在技术层面加强防火墙、加密存储、权限控制、区块链溯源等手段外，还应在制度层面建立严格的安全责任体系，明确各部门的职责边界与监督机制。同时，要定期开展系统安全演练与应急处置预案，确保一旦出现突发问题，能够在最短时间内完成隔离、修复和恢复，最大限度降低风险影响。

2 工程档案信息化管理中的主要安全风险

2.1 数据泄露与非法访问

工程档案信息具有高度敏感性，其中包含设计方案、施工技术参数、成本预算、供应链信息以及涉及合作方的商业秘密。一旦遭遇非法获取，不仅会造成直接的经济损失，还可能引发工程安全隐患，甚至影响企业在行业内的竞争力。目前，一些工程档案管理系统仍存在访问权限设置不合理、身份认证机制不完善等问题，导致内部人员可能越权访问敏感数据，或者外部黑客通过技术手段轻易突破防护壁垒。同时，加密措施薄弱、数据传输未采用端到端加密等，也增加了数据泄露的风险。若档案信息在流通过程中被截取或复制，不法分子可能利用这些资料进行投标操控、商业敲诈，甚至为工程质量造假提供条件。因此，如何通过严格的权限分级管理、强化加密手段和多重身份验证来确保档案数据的安全，是工程档案信息化管理亟需解决的重要课题。

2.2 信息篡改与伪造

工程档案的真实性和完整性是保障工程建设质量与安全的重要前提。档案一旦被篡改，可能导致责任追溯困难，甚至为违法违规行为提供掩护。黑客若利用系统漏洞对施工记录、检测报告、合同文本等关键数据进行篡改，不仅会破坏档案的公信力，还会在出现工程事故时，使调查过程难以准确还原真实情况，严重影响事故认定和责任划分。更有甚者，若工程质量检验数据被人为伪造，可能导致不合格工程进入使用阶段，埋下严重安全隐患。例如，某些施工环节的检测结果若被修改为合格，后续监管部门便可能在错误数据的掩护下放行，最终酿成安全事故。由此可见，档案信息篡改的危害具有长期性和隐蔽性，必须通过技术和制度双重防范，例如引入区块链技术确保数据的不可篡改性，建立日志追踪机制以记录所有操作行为，从而提升档案数据的安全性和权威性。

2.3 系统故障与数据丢失

信息化档案管理高度依赖硬件设备和网络环境，其稳定性直接决定了档案管理的安全性与可靠性。一旦服务器宕机、数据库损坏，或遭遇恶意攻击如勒索病毒，都可能导致大规模的数据丢失，给工程管理带来严重后果。尤其是在尚未建立完善的备份机制和灾备体系的情况下，数据恢复的难度极大，部分情况下甚至会造成永久性损失。大规模数据丢失不仅会影响工程的日常运行与决策，还可能在法律纠纷、事故调查中造成证据缺失，削弱企业和监管机构的公信力。

此外，系统故障往往具有突发性和不可预测性，管理部门在日常维护中如果缺乏定期检测与风险评估，容易在故障发生时陷入被动。例如，一些小型工程企业可能为了节约成本，忽视了系统冗余设计和异地备份部署，导致在遇到黑客攻击或自然灾害时，整个档案系统瘫痪，数据无法恢复。为此，必须在技术层面建立完善的多层次备份体系，定期对系统进行压力测试和漏洞修复；在管理层面制定严格的应急预案，确保出现突发情况时能够快速启动灾备机制，最大程度降低损失。

3 安全风险的成因分析

3.1 技术防护不足

在工程档案信息化管理过程中，技术防护是最基础、最直接的安全屏障。然而，部分档案管理系统在设计时过于追求功能的多样化与操作的便捷性，却忽视了安全机制的建设与更新。这种“重功能、轻安全”的思路，往往在无形中为潜在的安全风险埋下隐患。例如，一些系统没有建立多重身份验证机制，用户只需单一口令即可进入系统，极易被黑客破解或内部人员泄密；部分系统在数据传输中仍采用明文或低级加密协议，无法抵御窃听与中间人攻击；同时，系统漏洞修补不及时，补丁更新滞后，给恶意攻击者留下了可乘之机。随着大数据与云计算的广泛应用，档案数据的存储和传输规模不断扩大，任何微小的技术防护疏漏，都可能引发严重的连锁反应。因此，强化技术防护，建立完善的身份认证体系、端到端加密机制以及定期漏洞扫描与修补机制，是保障工程档案信息安全的关键。

3.2 管理制度缺陷

与技术问题相比，管理制度的缺陷往往更加隐蔽，却对档案安全具有长期的负面影响。在很多单位中，档案管理人员的安全意识不足，未能充分认识到信息化管理中潜在的风险，导致日常工作流于形式。例如，权限分配不科学，部分工作人员可以接触到超出其工作范围的敏感档案，增加了信息泄露的可

能性；缺乏有效的监督与审计机制，使得违规操作和越权行为难以及时发现和纠正。此外，目前在工程档案信息化管理方面，尚缺乏统一的行业规范和标准，不同单位在安全标准、权限设置、数据备份及灾备机制等方面存在明显差异，这种差异化不仅使档案安全缺乏统一保障，也加剧了风险的不确定性。随着工程项目跨地区、跨行业的合作增多，缺乏统一制度标准的问题将进一步放大，导致档案数据在流通环节的安全性难以保障。因此，建立科学、规范、统一的管理制度，提升档案人员的安全意识，配备完善的监督审计机制，是补齐管理短板的必然要求。

3.3 法律法规约束不足

法律法规是保障工程档案信息化安全的制度基石。近年来，国家相继出台了《档案法》《网络安全法》《数据安全法》等，为档案管理提供了法律依据。然而，在工程档案信息化管理的具体实践中，仍然存在执行不到位、标准细化不足、违规成本偏低等问题。一方面，现有法律在工程档案领域的针对性和可操作性不足，导致很多企业和单位在落实时存在模糊地带；另一方面，由于监管机制和处罚措施不够严格，部分单位在安全管理上抱有侥幸心理，往往以降低成本为由忽视必要的安全投入。这样的状况不仅使违规行为难以及时纠正，也使得档案安全风险难以从源头得到有效遏制。例如，在实际操作中，一些单位未能按照法律要求建立完善的备份与应急机制，但由于缺乏强制检查与处罚，问题长期存在却未被整改。由此可见，只有进一步细化和完善法律法规，明确工程档案信息化管理的安全标准，加大执法和处罚力度，才能真正发挥法律的约束与震慑作用。

4 防范工程档案信息化管理安全风险的措施

4.1 强化技术防护体系

应建立多层次的安全防护结构，包括数据加密、访问控制、入侵检测与防御系统等。利用区块链技术可实现档案的不可篡改性，确保信息溯源。与此同时，定期进行系统漏洞扫描与修补，保障平台长期稳定运行。

4.2 完善管理制度与监督机制

建立严格的权限管理体系，确保不同岗位人员只能在职责范围内操作相关档案。推行操作日志与审计制度，实现全过程可追溯。加强档案管理人员的安全培训，提升其风险意识和操作规范性。

4.3 健全法律法规与行业标准

应在现有法律法规基础上，出台专门针对工程档案信息化管理的安全规范，对责任分工、违规处罚及安全等级评定作出明确规定。通过提高违法成本和强化行业自律，推动安全管理制度化、规范化。

5 结语

工程档案信息化管理在提高效率和便利性的同时，也不可避免地引入新的安全风险。如何在便利与安全之间寻求平衡，是当前亟待解决的问题。本文从数据泄露、信息篡改、系统故障等风险入手，分析了成因，并提出了技术、管理和法律三方面的防范措施。未来，随着人工智能与区块链技术的进一步发展，工程档案的安全管理有望实现更高水平的智能化与可靠性。唯有在技术手段和制度建设双重保障下，才能真正发挥信息化管理的优势，确保工程档案的真实性、安全性与长久价值。

参考文献：

[1] 罗琳,亓丽,崔跃.浅谈信息化环境下建设工程档案管理的提升路径[J].黑龙江档案,2024,(04):82-84.

[2] 李惠天,邓君君.工程档案管理信息化建设探究[J].房地产世界,2024,(15):161-163.

[3] 廖燕.信息化背景下医院工程档案管理质量提升路径研究[J].兰台内外,2024,(11):22-24.

[4] 郑岚.信息化视域下建设工程档案管理提升策略[J].未来城市设计与运营,2024,(03):81-83.

[5] 张兰.浅谈工程档案管理信息化[J].办公室业务,2023,(14):127-129.

[6] 吕燚.档案信息化建设与工程档案管理措施分析[J].质量与市场,2021,(10):167-168.