

# 信息安全与档案保护：现代档案管理的关键问题

王境晨

秦皇岛市海港区人民检察院

**摘要：**在当今数字化时代，信息安全和档案管理的重要性愈发凸显。随着信息技术的不断发展和应用，组织所面临的安全威胁也日益复杂和多样化。特别是对于机关事业单位或高校图书馆等拥有大量敏感信息和重要档案的机构而言，确保这些信息和档案的安全性和完整性显得尤为重要。因此，本文就现代档案管理的关键问题展开论述，旨在确保档案数据的安全、完整和可用性，为组织的稳健发展提供可靠的保障。

**关键词：**信息安全；档案保护；关键问题；解决策略

【DOI】10.12252/j.issn.2096-627X.2022.08.168

## 一、档案的价值与保护需求

档案作为一种记录过去事件、管理信息和传承文化的载体，具有不可估量的价值。它们承载着机构、组织或个人的历史、活动和决策，是过去经验的积累和未来发展的基石。在档案管理中，理解档案的价值并确保其得到有效保护是至关重要的。档案具有历史价值。通过档案，可以了解过去的事件、人物和社会环境，从而更好地理解和把握历史的发展脉络。档案记录了机关的发展轨迹、决策过程和发展成就，为后人研究历史、进行文化传承提供了珍贵的资料和参考。另外，档案具有法律和证明价值，在法律程序中，档案被用作证据支持，对于解决纠纷、确认权利和义务等方面具有重要作用。档案的合法性、完整性和真实性对于其在法律程序中的有效性至关重要，因此保护档案的安全和完整性是维护司法公正和法治的基础。档案还具有行政管理和决策支持的价值。在机关事业单位或高校图书馆中，档案记录了重要的管理信息、政策文件和决策过程，为机构的日常运作和长远发展提供了依据和支持。有效管理和利用档案可以提高工作效率、优化资源配置，为机构的科学决策和管理提供重要参考。随着信息化和数字化的发展，档案面临着各种安全威胁和风险，如数据泄漏、篡改和灾害损失等。因此，建立健全的档案保护制度和安全管理机制势在必行。

## 二、信息安全对机关事业单位（或高校图书馆）档案管理的影响

信息安全对机关事业单位（或高校图书馆）档案管理具有重要影响，其影响体现在多个方面，如数据完整性、保密性、可用性等方面。信息安全对档案管理的影响体现在数据完整性方面，档案作为机构或高校图书馆的重要信息资产，其完整性直接关系到信息的可信度和可靠性。如果档案数据受到篡改或损坏，将严重影响到机关

单位或高校图书馆的决策、研究和管理工作的。因此，保障档案数据的完整性是信息安全工作的首要任务之一。再者，信息安全还对档案管理的保密性产生重要影响。在机关事业单位或高校图书馆中，有些档案可能涉及个人隐私、商业机密或国家安全等敏感信息，如果这些信息泄漏，将对机构或高校图书馆造成严重的损失和影响。因此，建立健全的信息安全保密制度和加密机制，对敏感档案进行严格管控和保护，是保障机关事业单位或高校图书馆档案管理安全的关键举措之一。此外，信息安全还影响到档案管理的可用性。机关事业单位或高校图书馆的档案管理工作需要随时随地对档案信息进行访问、查询和利用，以支持决策、研究和学习等工作。如果档案信息受到病毒攻击、网络故障或数据丢失等问题影响，将严重影响到档案管理的正常运作和服务效率。因此，确保档案信息的可用性，是信息安全工作的又一重要目标。

## 三、现代档案管理中的关键问题

现代档案管理面临着诸多关键问题，这些问题涉及数字化转型、信息安全、档案保护与风险管理、法律合规等方面，对于确保档案的完整性、保密性和可用性具有重要影响。数字化档案管理是现代档案管理的关键问题之一。随着信息技术的不断发展，越来越多的档案被数字化存储和管理，以提高档案检索、共享和利用的效率。然而，数字化转型也带来了诸多挑战，包括数据格式标准、长期保存、数字鉴别和数字安全等方面的问题。因此，如何有效进行数字化档案管理，是现代档案管理中亟待解决的重要问题之一。同时，信息安全策略是现代档案管理的另一关键问题。随着网络技术的普及和信息化程度的提高，档案面临着来自网络攻击、数据泄漏和信息篡改等安全威胁。因此，建立健全的信息安全策略和安全管理机制，加强对档案数据的保护和监控，是保障档案管理安全的重要举措。此外，档案保护

与风险管理也是现代档案管理的关键问题之一。档案管理工作面临着各种风险，如自然灾害、人为破坏、数据丢失等，对档案的安全性和完整性构成威胁。因此，建立完善的档案保护机制和灾害恢复计划，进行风险评估和预防，是保障档案长期保存和有效利用的重要手段。最后，法律合规要求也是现代档案管理的关键问题之一。随着法律法规的不断完善和加强，档案管理工作面临着越来越严格的法律合规要求，包括隐私保护、数据安全、信息公开等方面的规定。因此，建立符合法律合规要求的档案管理制度和流程，加强对法律法规的学习和遵守，是确保档案管理工作合法合规的关键举措。

#### 四、提升信息安全与档案保护的策略

##### 1、建立健全的安全政策和制度

建立健全的安全政策和制度对于保障组织的信息安全和档案保护至关重要。这一政策和制度应该包括一系列明确的规定和措施，以确保组织内部人员了解并遵守其在信息安全和档案保护方面的责任和义务。明确的信息安全政策应该涵盖组织对于信息安全的整体目标和原则，包括保护档案不受未经授权的访问、确保档案数据的完整性和保密性、遵守相关法律法规等。这些政策应该与组织的整体战略和目标相一致，并得到高层管理层的支持和承诺。另外，明确的档案保护制度应该包括具体的实施措施和操作规范。这些规范可能包括权限管理、数据访问控制、密码策略、备份与恢复规范等。通过合理的权限管理和数据访问控制机制，确保只有授权人员才能访问和操作相应的档案数据；同时，采取严格的密码策略和定期备份与恢复规范，以提高系统的安全性和数据的可靠性。

##### 2、加强机关单位培训和意识教育

通过定期的培训和教育活动，可以提高机关单位对信息安全和档案保护的认识水平，增强其对安全风险的警惕性，从而有效地减少安全事件和数据泄露的发生。培训内容应该涵盖对信息安全和档案保护的基本概念和原则的介绍。机关单位需要了解什么是信息安全，为什么信息安全对组织至关重要，以及档案保护在整个信息安全体系中的重要性。通过这些基础知识的传授，可以让机关单位认识到安全工作的重要性，并树立正确的安全意识。其次，培训应该重点关注当前常见的安全威胁和攻击手段。这包括社会工程学攻击、网络钓鱼、恶意软件等常见的安全威胁。机关单位需要了解这些威胁的工作原理、识别特征以及防范方法，以增强其对安全威胁的识别和防范能力。通过实际案例的讲解和模拟演

练，可以帮助机关单位更好地理解 and 应对各种安全威胁。另外，培训还应该针对不同岗位和职责的机关单位制定相应的培训计划。不同岗位的机关单位面临的安全风险和威胁可能有所不同，因此培训内容需要根据其实际工作需求进行定制化。对于系统管理员和IT人员，培训内容可以更加深入地涉及技术层面的安全知识和操作技巧；而对于普通机关单位，培训内容则更多地侧重于基础的安全意识和实用的防范方法。此外，培训应该是一个持续的过程，而不是一次性的活动。随着安全威胁的不断演变和发展，机关单位的安全意识和知识也需要不断更新和提升。因此，组织应该建立起定期的培训机制，定期组织机关单位参加安全培训和教育活动，以保持其安全意识的敏感性和及时应对新威胁的能力。

##### 3、加密和安全传输

加密和安全传输在现代信息安全和档案保护中扮演着至关重要的角色。这两项技术不仅可以保护敏感信息和重要档案的安全性，还可以防止数据在传输过程中被窃取或篡改，从而确保数据的保密性、完整性和可用性。加密技术是保护敏感信息和重要档案安全的关键手段之一。通过加密技术，可以将原始的明文数据转换成密文，只有授权的用户才能够解密并获得原始数据。对于敏感信息和重要档案，可以使用强加密算法对其进行加密保护，以防止未经授权的访问和窃取。其中，安全传输是保障数据在传输过程中不受攻击和篡改的重要手段。在数据传输过程中，数据可能会经过不安全的网络环境，容易受到黑客攻击、窃取或篡改。为了确保数据的安全传输，可以采用安全传输协议和加密通信通道。常见的安全传输协议包括SSL/TLS，它可以在数据传输的过程中使用加密技术，确保数据在传输过程中不被窃取或篡改。另外，还可以采用数字证书和数字签名技术来确保数据传输的安全性。数字证书可以验证通信双方的身份和信任关系，防止中间人攻击；数字签名可以确保数据的完整性和真实性，防止数据在传输过程中被篡改。

##### 4、建立灵活的权限管理系统

建立灵活的权限管理系统是确保信息安全和档案保护的重中之重，通过根据机关单位的工作职责和需求，分配适当的访问权限，可以有效地限制对敏感档案和信息的访问，减少不必要的风险和泄漏可能性。同时，实施严格的身份验证和访问控制机制，确保只有授权人员能够访问和修改档案数据，进一步加强了档案管理的安全性和保护措施。为此，应建立灵活的权限管理系统需

要根据组织内部的岗位和职责情况，确定不同机关单位对档案和信息的访问需求。通过对机关单位的工作职责和需求进行详细的了解和分析，可以制定出相应的权限分级制度，确保每个机关单位都能够获得所需的访问权限，同时又不会给系统安全带来风险。同时，实施严格的身份验证和访问控制机制是确保权限管理系统有效运行的关键。通过采用多因素身份验证方式，如密码、指纹、智能卡等，可以有效地确认用户的身份，并防止未经授权的人员获取访问权限。同时，建立访问控制列表和审计日志，记录每次访问的详细信息，及时发现异常行为和安全威胁。除此之外，对于敏感档案和信息，可以采用更加严格的访问控制策略。例如，实施基于角色的访问控制，将访问权限与机关单位的职责和角色相匹配，确保只有具有相应权限的人员才能够访问和修改敏感档案。同时，对于一些特殊情况，如临时授权访问、异常访问行为等，需要建立相应的审批流程和应急响应机制，及时处理和管理。最后，建立灵活的权限管理系统需要不断地进行监控和改进。随着组织内部人员和业务需求的变化，权限管理系统也需要及时调整和优化，确保系统的适用性和有效性。定期进行权限审查和访问审计，发现和纠正潜在的安全风险和漏洞，提高系统的安全性和保护水平。根据机关单位的工作职责和需求分配适当的访问权限，实施严格的身份验证和访问控制机制，可以有效地保护敏感档案和信息，防止未经授权的访问和操作，提高档案管理的安全性和保护水平。

#### 5、定期的安全审计和检查

定期的安全审计和检查是确保信息安全和档案保护持续有效的有力保障，通过建立定期的安全审计制度，可以对档案管理系统和安全措施进行全面检查和评估，发现潜在的安全漏洞和风险，及时采取措施加以修复和改进，从而提高档案管理的安全性和保护水平。相关机关单位必须要定期的进行安全审计，同时，需要确立明确的审计目标和范围，这包括确定审计的时间周期、审计的具体内容和范围，以及参与审计的人员和机构。审计范围应该涵盖档案管理系统的各个方面，包括系统架构、数据存储、访问控制、安全策略等，以确保全面了解系统的安全状况。其次，安全审计应该采用多种审计方法和工具，以确保审计的全面性和有效性。这包括系统漏洞扫描、安全策略检查、日志分析、安全风险评估等多种审计手段。通过综合运用这些审计方法和工具，可以全面了解系统的安全状况，发现潜在的安全隐患和风险。另外，安全审计应该注重审计结果的

分析和评估，发现安全漏洞和风险后，需要对其进行及时的分析和评估，确定其严重程度和影响范围，并制定相应的修复和改进措施。同时，需要对审计结果进行归档和记录，以备后续审计和复审之用。最后，安全审计的结果应该及时通报和反馈给相关部门和专业的团队进行处理。发现的安全漏洞和风险应该及时向相关责任人报告，并要求其采取必要的措施加以修复和改进。同时，还应该建立起定期的审计报告和汇总机制，向高层管理层和相关利益相关方汇报审计结果，加强对信息安全和档案保护工作的监督和管理。不难看出，通过定期的安全审计和检查是确保信息安全和档案保护持续有效的的重要举措。通过建立明确的审计目标和范围，采用多种审计方法和工具，注重审计结果的分析和评估，以及及时通报和反馈审计结果，可以有效发现和解决安全漏洞和风险，提高档案管理的安全性和保护水平。

#### 结束语

综上所述，在信息安全和档案保护工作中，需要不断学习和探索，积极应对不断变化的安全威胁和挑战，确保组织档案数据的安全、完整和可用性。只有加强安全意识，建立起健全的安全制度和措施，才能真正保障组织档案数据的安全性，为组织的可持续发展提供坚实的保障。让我们共同努力，共同守护好组织的信息宝库，共创信息安全的美好未来。

#### 参考文献

- [1] 钱德凤. 后保管时代数据资源档案化模式探析——以人事档案管理实践为例[J]. 内蒙古科技与经济, 2023, (16): 36-39+43.
- [2] 秦长森. 我国档案安全刑法保护的回顾、反思与完善[J]. 档案学研究, 2023, (04): 57-64.
- [3] 孙建军, 马亚雪. 面向多元场景的数据治理: 进展与思考[J]. 图书与情报, 2023, (04): 1-11.
- [4] 徐瞰. 电子数据保管链制度的价值基础及其建构进路[J]. 湖南社会科学, 2023, (04): 121-131.
- [5] 郝阳. 人工智能技术在医院档案管理中的应用与展望[J]. 办公自动化, 2023, 28(15): 54-57.
- [6] 刘文钰. 我国公共图书馆文旅融合服务现状研究[D]. 山西大学, 2023.

作者简介: 王境晨, 单位: 秦皇岛市海港区人民检察院, 出生年月日: 1987.3.14, 性别: 男, 民族: 汉, 籍贯: 河北省秦皇岛市, 学历: 本科, 职称: 助理馆员, 研究方向: 档案管理。