 DOI: https://doi.org/10.12345/daglyqyfzyj.v2i6.18767

Personnel File Information Security Risk Assessment and Prevention Strategy

Yi Liu

Dianjiang Mental Health Center, Chongqing, 408300, China

Abstract

With the rapid progress of information technology, the information management of personnel files has become an indispensable part of the efficient operation of modern organizations. However, the problem of information security has also become prominent, and the risks of data leakage, tampering and loss pose a serious threat to the rights and interests of individuals and organizations. This paper deeply discusses the core role of personnel file information security in organizational operation, and systematically analyzes the main security challenges faced at present. To address these challenges, this paper proposes a series of comprehensive prevention strategies, including strengthening the awareness of data protection, improving the system security management system, implementing strict permission control, enhancing physical security protection measures, developing a comprehensive disaster preparedness and recovery plan, and strengthening personnel management and training. These strategies aim to comprehensively reduce the risk of personnel file information security, ensure the security and integrity of personal and organizational information, and provide a solid guarantee for the sustainable development of the organization.

Keywords

personnel files; information security; risk assessment; preventive strategy

人事档案信息安全风险评估与防范策略

刘毅

垫江县精神卫生中心，中国·重庆 408300

摘　要

随着信息技术的迅猛进步，人事档案材料的信息化管理已成为现代组织高效运作不可或缺的一环。然而，信息安全问题也随之凸显，数据泄露、篡改和丢失等风险对个人和组织权益构成严重威胁。论文深入探讨了人事档案信息安全在组织运营中的核心作用，并系统分析了当前面临的主要安全挑战。为应对这些挑战，论文提出了一系列综合性的防范策略，包括强化数据保护意识、健全系统安全管理体系、实施严格的权限控制、增强物理安全防护措施、制定全面的灾备与恢复计划，以及加强人员管理与培训。这些策略旨在全面降低人事档案信息安全风险，确保个人与组织信息的安全与完整，为组织的可持续发展提供坚实保障。

关键词

人事档案；信息安全；风险评估；防范策略

1 引言

在信息技术日新月异的时代背景下，人事档案信息安全问题已不容忽视。作为组织和个人信息的核心组成部分，人事档案的保密性、完整性和可用性对于保护个人隐私、确保组织决策的科学性以及维护组织声誉至关重要。因此，对当前人事档案信息安全状况进行深入的风险评估，并据此制定切实可行的防范策略，对于提升整体信息安全水平、保障各方利益具有迫切而深远的意义。

【作者简介】刘毅（1977–），女，中国重庆人，助理馆员，从事人事档案管理研究。

2 人事档案信息安全的作用

2.1 保护个人隐私

在信息化时代，个人隐私的保护显得尤为重要[1]。人事档案中存储了大量关于个人的敏感信息，包括但不限于姓名、身份证号、家庭住址、联系方式、教育背景、工作经历等。这些信息一旦泄露，可能被不法分子利用，对个人造成财产损失、身份盗窃、骚扰甚至更严重的后果。因此，保障人事档案信息安全的首要任务就是保护个人隐私，防止个人信息被非法获取和滥用，确保个人的合法权益不受侵害。

2.2 确保组织决策的准确性

人事档案是组织进行人力资源管理的重要依据，记录了员工的基本信息、教育背景、工作经历、绩效表现等关键数据，是组织在招聘、选拔、晋升、培训等各个环节中进行

决策的重要参考。如果人事档案信息不安全，存在被篡改或伪造的风险，那么组织在决策时就可能基于错误的信息，导致决策失误，影响组织的运营效率和发展方向。因此，保障人事档案信息安全，可以确保组织在决策过程中使用准确、可靠的信息，提高决策效率和质量，为组织的持续发展提供有力保障。

2.3 维护组织声誉

人事档案信息安全不仅关系到个人隐私和组织决策的准确性，还关系到组织的声誉和形象。一个组织如果无法保障其人事档案信息的安全，一旦发生信息泄露或滥用事件，将给组织带来极大的负面影响。这些信息可能包括组织的商业机密、客户资料、员工隐私等敏感信息，一旦泄露，将严重损害组织的声誉和形象，影响组织的公信力和市场竞争力。因此，保障人事档案信息安全是维护组织声誉的重要措施之一，对于提升组织的品牌形象和公信力具有重要意义。

3 人事档案信息安全存在的问题

3.1 数据泄露风险

数据泄露是人事档案信息安全面临的重要风险之一，由于系统漏洞、网络攻击或内部人员的不当操作等原因，人事档案信息可能被非法获取和泄露 [2]。数据泄露不仅会导致个人隐私的泄露，还可能被不法分子用于身份盗窃、电信诈骗等非法活动，对个人造成极大的困扰和损失。对于组织而言，数据泄露可能暴露组织的商业机密、客户资料等重要信息，对组织的声誉和利益造成严重影响。

3.2 数据篡改风险

数据篡改是另一个需要高度关注的问题，恶意攻击者或内部不法分子可能利用技术手段或内部权限，对人事档案进行非法篡改。这种篡改可能导致信息的真实性和完整性受损，使组织在决策过程中基于错误的信息，从而影响决策的准确性。更为严重的是，篡改的人事档案信息如果被用于法律诉讼或争议解决中，可能引发法律纠纷，给组织带来法律风险。

3.3 数据丢失风险

数据丢失是人事档案信息安全中另一个常见的风险，硬件故障、自然灾害、人为失误等因素都可能导致人事档案信息的丢失。数据丢失不仅会给组织带来巨大的经济损失，还可能影响组织的正常运营。例如，如果员工的人事档案丢失，组织可能无法准确了解员工的个人信息、工作经历和绩效表现，从而影响招聘、晋升等决策的准确性。此外，如果组织的客户资料、商业机密等重要信息丢失，还可能对组织的声誉和竞争力造成严重影响。

4 人事档案信息安全的防范策略

4.1 加强数据保护意识

在信息时代，数据保护意识对于保障人事档案信息安全至关重要 [3]。组织应重视员工的数据保护意识培养，通过定期的信息安全培训和教育活动，使员工深刻认识到保护信息的重要性。培训内容应涵盖信息安全基础知识、个人隐私保护、信息安全风险识别与应对等方面，以提高员工对信息安全问题的敏感性和防范能力。通过培训，员工能够认识到自己在保护信息中的责任，明白泄露或滥用个人或组织信息的严重后果。员工将学会识别和避免潜在的信息安全风险，如识别网络钓鱼邮件、避免在公共网络上进行敏感操作等。在处理人事档案信息时，员工将始终遵循安全规范，确保信息的安全性和完整性。

例如，某大型公司与信息安全培训机构携手，为员工定制专属课程，既涵盖网络安全基础知识，又针对公司业务系统及数据特点教授风险识别与防范方法。为提高员工对网络钓鱼邮件的警惕性，公司定期组织模拟钓鱼邮件识别演练，并对未能及时识别的员工给予反馈和指导。此外，公司还创办了信息安全知识竞赛，以赛促学，激发员工的学习热情。在工作坊中，员工能亲自参与安全操作流程的实践，如学习正确配置和使用加密软件，以确保敏感信息的安全性。公司还专门设立“信息安全意识周”，期间举办各类活动，如讲座、海报设计比赛等，增强员工的信息安全意识。

4.2 完善系统安全管理

系统安全管理是确保人事档案信息安全的关键环节，组织应采用先进的安全技术，如防火墙、入侵检测系统等，以建立多层次的安全防护体系，防止外部攻击和数据泄露。这些安全技术能够实时监测和防御网络威胁，及时发现并阻止潜在的安全风险。此外，组织应定期对系统进行安全检查和更新，及时修补漏洞和缺陷，确保系统的稳定性和安全性。同时，建立严格的信息安全管理制度，明确信息安全管理的职责和要求，确保各项安全措施得到有效执行。这包括制定信息安全政策、建立安全事件响应机制、定期进行安全演练等。就某公司而言系统安全管理是确保人事档案信息安全的关键环节，组织应采用先进的安全技术，如防火墙、入侵检测系统等，以建立多层次的安全防护体系，防止外部攻击和数据泄露。这些安全技术能够实时监测和防御网络威胁，及时发现并阻止潜在的安全风险。同时，组织应定期对系统进行安全检查和更新，及时修补漏洞和缺陷，确保系统的稳定性和安全性。再建立严格的信息安全管理制度，明确信息安全管理的职责和要求，确保各项安全措施得到有效执行。

4.3 严格权限管理

权限管理是保障人事档案信息安全的重要手段，组织应建立完善的权限管理制度，根据员工的职责和需要，授予不同的访问和操作权限。通过严格的权限控制，可以确保只有经过授权的人员才能访问和修改人事档案信息，防止信息被非法获取和篡改。同时，实施访问控制和审计机制，对所有对档案信息的访问和操作行为进行监控和记录。这有助于及时发现和应对潜在的安全风险，确保信息的准确性和完整性。例如，某大型公司为不同职责的员工设定了明确的访问权限，如只读权限和编辑权限。而且，该公司采用先进的访

问控制系统，实时监控所有档案信息的访问和操作行为，并详细记录在案。

4.4 加强物理安全防护

物理安全防护是确保人事档案信息安全的重要保障，组织应选择安全可靠的存储设备，建立安全的存储环境，如设置专门的档案室、安装监控摄像头等，以防止非法侵入和破坏[4]。同时，限制非授权人员进入档案室，确保只有经过授权的人员才能接触和操作人事档案。此外，建立监控和报警系统，及时发现和解决安全风险，确保档案信息的物理安全。

比如，某大型公司选用了经过权威认证的防磁硬盘和防火存储柜，这些设备的耐用性和稳定性得到了广泛认可，有效抵抗自然灾害和人为破坏。同时，公司建设了符合安全标准的档案室，配备了先进的门禁系统和监控系统，确保档案室的安全。门禁系统采用生物识别技术，如指纹识别或面部识别，确保只有经过授权的人员才能进入。监控系统则实现了全天候无死角监控，所有进入档案室的人员及其活动都被记录下来。此外，公司在档案室内外安装了高清监控摄像头，并部署了红外感应器和烟雾探测器等设备。这些设备与监控中心相连，一旦发生异常情况，如入侵、火灾等，系统会立即发出警报，并通知安保人员进行处理。据统计，自从实施这些措施以来，档案室的非法入侵事件减少了 90%，火灾事故为零，有效地保障了人事档案的信息安全。

4.5 制定灾备和恢复计划

灾备和恢复计划是应对突发事件和灾难性事件的关键措施，组织应建立备份机制，定期对人事档案进行备份，并将备份数据存储在安全可靠的地方，以防止数据丢失和损坏。同时，制定详细的灾难恢复计划和应急响应机制，明确在发生意外情况时如何快速恢复数据和服务。通过灾备和恢复计划的制定和实施，组织能够在最短时间内恢复人事档案信息的完整性和可用性，确保组织的正常运营。

例如，某大型公司每季度对人事档案进行一次全面备份，并将备份数据存储在位于异地的安全数据中心，以避免因自然灾害或硬件故障导致的数据丢失。为了提高恢复效率，公司详细规划了灾难恢复流程，包括数据恢复、系统重建和网络恢复等环节。同时，建立了应急响应机制，明确了在发生灾难时的责任分工和操作流程。在一次模拟灾难恢复演练中，从发现故障到恢复数据服务，整个过程仅用时 2 小时，远低于预设的 4 小时目标，展现了高效的应急响应能力。

4.6 加强人员管理和培训

档案管理人员是保障人事档案信息安全的重要力量，组织对档案管理人员进行专业培训和教育，提高档案管理人员的业务素质和管理能力。通过培训，档案管理人员能够掌握先进的信息安全技术和管理方法，提高处理信息安全问题的能力。同时，建立考核和激励机制，对档案管理工作进行定期评估和奖惩，提高档案管理人员的工作积极性和责任心。通过加强人员管理和培训，组织能够建立一支高效、专业的档案管理团队，为人事档案信息安全提供有力保障。

例如，某大型公司与一家权威的网络安全培训机构携手，为 50 名档案管理人员提供了一场为期三个月的专业培训。课程内容全面覆盖信息安全基础、数据加密技术以及档案管理系统操作等关键领域。培训采用理论与实操相结合的模式，确保学员能够扎实掌握所学。在培训期间，学员们共参与了 20 场实战演练，平均每人完成了 10 个信息安全项目，以巩固所学知识。此外，培训机构还进行了 5 次模拟考试，学员的平均成绩从培训前的 60 分跃升至 85 分，增幅高达 41.7%，显示出培训效果显著。为了持续激励档案管理人员，公司构建了一套科学的考核与激励机制。每个季度，都会对档案管理人员的绩效进行细致评估，并根据评估结果实施奖惩。对于表现突出的员工，公司不仅给予奖金，还提供晋升机会。而对于需要提升的员工，则提供针对性的培训与支持。自激励机制实施以来，档案管理人员的整体工作效率提升了 25%，成效明显。

5 结语

人事档案信息安全是组织运营中不可忽视的一环。通过加强数据保护意识、完善系统安全管理、严格权限管理、加强物理安全防护、制定灾备和恢复计划以及加强人员管理和培训等防范策略的实施，可以有效降低人事档案信息安全风险，保障个人和组织的权益。在未来的工作中，信息安全团队将继续关注人事档案信息安全问题，不断完善和优化防范策略，以应对新的挑战和威胁。

参考文献

[1] 段玉玲,侯德山.数字化人事档案的信息安全保障研究[J].无线互联科技,2019,16(22):13-14.

[2] 黄芳心.人事档案信息在网络中运行的安全风险与对策[J].开放潮,2006(Z2):46-47.

[3] 项文新.基于信息安全风险评估的档案信息安全保障体系构架与构建流程[J].档案学通讯,2012(2):87-90.

[4] 项文新.构建基于信息安全风险评估的档案信息安全保障体系必要性研究[J].档案学通讯,2008(1):56-59.