档案信息安全管理在事业单位中的重要性与对策探讨

王　辉

兴安盟纪委 内蒙古 兴安盟 137400

【摘　要】：档案信息作为事业单位履行职能、开展业务的核心数据资产，其安全管理直接关系到公共利益、数据真实性与单位合规运营。本文从公共服务保障、数据资产保护、合规经营、业务延续性四个维度分析档案信息安全管理的核心重要性，针对系统存在的突出问题，提出相关的完善对策。研究成果为事业单位优化档案信息安全管理模式提供实操性支撑，对推动事业单位档案管理数字化、安全化发展具有重要意义。

【关键词】：事业单位；档案信息安全；安全管理；风险防控；对策探讨

DOI:10.12417/3041-0630.25.24.031

1 档案信息安全管理在事业单位中的核心重要性

1.1 保障公共服务连续性与公信力

事业单位的档案信息直接关联公共服务的开展，如民生保障类档案、公共项目档案、政策执行档案等，是服务群众、推进工作的重要依据。档案信息安全受损会导致公共服务流程中断、决策依据失真，影响服务质量与效率；若涉密档案泄露，还会损害政府公信力与公共利益，引发社会风险。

1.2 保护核心数据资产与知识产权

事业单位在长期运营中形成的科研成果、技术方案、项目报告、专利资料等档案信息，是单位核心知识产权与数据资产的重要组成部分。此类档案信息的安全直接关系到单位的创新发展与竞争力，若发生泄露或篡改，可能导致科研成果流失、项目利益受损，甚至引发知识产权纠纷，造成不可挽回的经济与声誉损失。

1.3 支撑单位决策与历史传承

档案信息记录了事业单位的发展历程、业务数据、经验教训，是单位制定发展规划、优化决策的重要参考。安全、完整的档案信息能为决策提供真实可靠的历史数据支撑，帮助单位规避风险、提升决策科学性；同时，档案作为单位历史传承的重要载体，其安全管理能确保单位历史沿革、文化积淀、工作成果的有效留存，为后续工作提供借鉴。

2 事业单位档案信息安全管理现存问题

2.1 思想认识不足，安全意识淡薄

部分事业单位管理层对档案信息安全重视不够，将档案管理视为“辅助性工作”，投入的人力、物力、财力不足，未将档案信息安全纳入单位整体安全管理体系。工作人员安全意识薄弱，存在“重使用轻保护”的误区，如随意借阅档案不登记、涉密档案擅自复印、电子档案未加密传输、账号密码共用等违规行为，人为引发安全风险。

2.2 技术防护薄弱，安全保障不足

纸质档案存储环境不符合要求，易导致档案霉变、损坏、丢失；电子档案存储未采用加密技术，传输过程中未建立安全通道，存在数据泄漏风险。档案管理系统未定期更新升级，存在安全漏洞；服务器、计算机等设备老化，未安装正版杀毒软件、防火墙，易遭受病毒入侵与网络攻击。电子档案未建立“本地+异地”双重备份体系，备份频率低、备份数据不完整；缺乏专业的恢复测试，发生数据丢失后无法快速有效恢复。

2.3 管理制度不健全，责任落实不到位

未结合单位实际制定《档案信息安全管理办法》《电子档案安全管理规范》《涉密档案管理细则》等专项制度，或制度内容笼统，缺乏可操作性。未建立“一把手总负责、分管领导牵头、档案部门具体落实、各业务部门协同配合”的分级责任体系，档案安全管理责任未分解到具体岗位与个人，出现问题后相互推诿。档案的收集、整理、保管、借阅、销毁等环节缺乏标准化流程，如借阅登记不完整、涉密档案审批权限不清晰、销毁流程不规范，易导致档案流失或泄露。

2.4 应急处置滞后，风险应对能力不足

多数事业单位未针对档案信息泄露、丢失、篡改、系统故障等安全事件制定应急预案，或预案内容笼统，未明确应急处置流程、责任分工、技术措施。未定期开展档案信息安全应急演练，工作人员对突发事件的处置流程、应对方法不熟悉，风险应对能力薄弱。

3 事业单位档案信息安全管理的优化对策

3.1 强化思想引领，提升安全意识

将档案信息安全管理纳入事业单位年度工作重点与绩效考核体系，与业务工作同规划、同部署、同落实；定期召开档案信息安全工作会议，分析安全形势，解决突出问题。加大资金投入，用于档案安全设施升级、技术防护系统建设、人员培

训等，为档案信息安全管理提供坚实保障。针对不同岗位开展差异化宣传，如对档案管理人员重点培训安全管理规范，对业务部门人员重点培训档案借阅与使用安全，对涉密人员重点培训保密纪律与责任。

3.2 筑牢技术防线，构建全面的技术防护体系

改善档案库房环境，配备恒温恒湿设备、防火报警器、防盗监控、气体灭火系统；涉密档案单独存放于密码保险柜或专用涉密库房，实行双人双锁管理。采用 AES-256 加密算法对电子档案进行存储加密，敏感数据采用“加密存储+访问授权”双重保护；电子档案传输采用 SSL/TLS 加密通道，禁止通过微信、QQ 等非安全渠道传输涉密或敏感档案；选用具备安全认证的正版档案管理系统，定期进行漏洞扫描与版本升级，安装入侵检测系统与入侵防御系统，防范网络攻击。所有接入档案管理系统的计算机、服务器均安装正版杀毒软件、防火墙，开启自动更新与病毒查杀功能；禁用不必要的端口与服务，设置复杂密码并定期更换。

3.3 健全制度体系，规范管理流程

结合单位实际，制定《档案信息安全管理总则》《纸质档案安全管理办法》《电子档案安全管理规范》《涉密档案管理细则》《档案借阅与销毁管理规定》等专项制度，明确各环节安全要求。对制度中的关键条款进行细化，如明确档案保密等级划分标准、不同等级档案的存储方式与访问权限、电子档案加密与备份要求等，确保制度可操作、可执行。制定档案信息安全责任追究办法，对因失职渎职导致档案安全事故的，按情节轻重给予通报批评、绩效考核降级、纪律处分等处罚；构成犯罪的，依法追究刑事责任。制定档案销毁清单，经分管领导与档案部门联合审核后，报单位主要领导批准；销毁过程实行双人监督，采用粉碎、彻底删除并覆盖数据的方式，做好销毁记录并存档。

3.4 提升人员能力，打造复合型的人才队伍

配备专职档案管理人员，明确岗位职责与任职条件，优先选拔具备档案管理、网络安全、计算机技术等专业背景的复合型人才；涉密档案管理岗位实行“持证上岗+政治审查”制度，确保人员可靠。建立人员稳定性保障机制，减少档案管理人员频繁变动；确需变动的，必须做好工作交接，签订保密承诺书，明确离岗后的保密责任。将档案信息安全管理能力纳入档案管理人员绩效考核，考核指标包括制度执行情况、安全事件发生率、专业技能水平等；对表现优秀的人员给予表彰奖励，对考核不合格的进行离岗培训或调整岗位。

3.5 完善应急机制，提升风险应对与处置能力

明确档案信息安全事件分类、应急组织机构与职责、应急处置流程、技术措施、应急资源保障等。应急预案经专家评审后发布实施，每年结合实际情况更新 1 次，确保与单位发展、技术升级、风险变化适配。配备备用服务器、移动硬盘、数据恢复工具、加密设备等技术应急设备；档案库房配备应急照明、灭火器、应急通道、防水设施等；涉密档案库房配备备用密码保险柜。组建由档案管理人员、技术人员、安全管理人员组成的应急处置队伍，明确各成员职责，确保事件发生后能快速响应。

4 结论

档案信息安全管理是事业单位履行公共服务职能、保障合规运营、保护核心资产的重要基础，是一项系统性、全流程的长期工作。当前事业单位在档案信息安全管理中仍存在思想认识不足、技术防护薄弱、制度不健全、人员素养不足、应急处置滞后等突出问题，需通过强化思想引领、筑牢技术防线、健全制度体系、提升人员能力、完善应急机制的五维对策，构建全方位、多层次的安全管理体系。

参考文献：

[1] 高琛琛.档案开放与信息安全管理的实践探索[J].黑龙江档案,2025,(04):188-190.

[2] 梁震洲,米伟南.基于大数据的档案信息安全管理系统设计[J].信息记录材料,2025,26(07):170-172.

[3] 李晓雪.企业档案信息安全管理的现状与对策[J].现代企业文化,2025,(10):40-42.