# 事业单位涉密档案管理风险防控措施

吴浩

国家广播电视总局二八一台，云南昆明，650212；

**摘要：**事业单位涉密档案管理风险防控效果与自身稳定发展、公共利益和国家秘密安全等密切相关，需加强对涉密档案管理的重视，注重全程管控、分类管理，合理划分各项权责，将风险防控工作落实到位，这是提高风险防控水平的关键。本文首先分析了事业单位涉密档案管理风险类型和风险成因，提出了完善制度体系、规范管理流程、优化环境技术条件、加强人员管理、健全监督机制等风险防控措施，以期为事业单位涉密档案管理风险有效防范提供参考。

**关键词：**事业单位；涉密档案；全流程管理；风险防控

**DOI：**10.69979/3041-0673.26.04.038

涉密档案管理是一项严谨性、系统性工作，这类档案管理全生命周期各环节均存在诸多风险隐患，尤其在档案管理数字化转型阶段，信息化技术应用在提升档案管理效率的同时，也带来了安全风险。为保障事业单位涉密档案安全，避免档案资料丢失、泄露、被篡改引发的严重后果与社会影响，应构建涉密档案管理风险防控体系，制定多层次风险防控措施，这对事业单位涉密档案的安全管理与利用具有重要意义。

## 1 事业单位涉密档案管理风险

涉密档案形成过程中，秘密等级界定不准确，涉密内容标注不规范；收集过程中涉密材料不完整、原件与复印件内容不一致、审查手续执行不到位；存储阶段，库房安全设施不完善、涉密档案与非涉密档案混合存储、电子存储介质随意存放、未进行加密处理、云端存储时安全防护不到位；档案利用与借阅环节，利用审批流程不严格、借阅范围和时间无限制、借阅手续不完整、涉密档案带出指定区域使用，导致涉密信息扩散；档案流转和移交环节，未进行密封包装或未采取专人护送、档案移交时未严格审核接收方资质、移交清单不详细、保密协议未签订，容易出现档案丢失现象；档案销毁环节，销毁流程不规范，存在随意丢弃问题，未彻底粉碎或消磁，没有进行全程监督，可能出现非法回收利用情况，造成信息泄露；电子涉密档案未部署安全管理技术、传输过程未加密、存储设备安全检测不及时，易遭受黑客攻击和病毒入侵，涉密档案被窃取。

## 2 事业单位涉密档案管理风险成因分析

### 2.1 制度体系不完善

事业单位涉密档案管理工作的有序开展需要完善的管理制度提供支持，但部分事业单位未结合自身实际制定针对性的涉密档案管理细则，缺乏相应管理制度和标准，仅参照普通档案法律法规执行，导致制度的可操作性不强。而且涉密档案管理制度内容不全面，未能充分考虑到档案全生命周期管理环节，实际管理中存在漏洞，无法及时发现涉密档案管理期间的风险隐患。实施的档案管理制度也未能及时更新，导致制度体系相对落后，难以快速适应信息化发展和新形势下的保密要求。制度执行过程中也缺乏约束管控条件，导致管理制度执行不到位，存在流于形式的问题。

### 2.2 顶层设计不合理

涉密档案管理中未能基于档案特点和管理需求进行合理顶层设计，导致涉密档案管理流程和利用指导标准不完善，难以为事业单位涉密档案管理工作的规范有序开展提供指导，日常管理中相关操作不规范。同时，涉密档案全生命周期管理要求、风险防控标准和操作规范不明确，难以实现全程闭环管理，无法及时发现各环节中的漏洞。另外，缺少分级分类管理标准，对于不同类型、不同等级的涉密档案，采用的管理要求和方式没有明确区分，未能结合不同类型涉密档案的特点制定针对性的防控策略，难以实现对各类风险的精准防控。

### 2.3 环境条件建设不足

部分事业单位管理涉密档案时，因管理经费有限或者涉密档案数量较少，没有加强涉密档案管理的信息化建设，通常采用普通档案的管理方式，对于电子涉密档案也缺乏加密和访问控制，相关管理系统功能单一，在出现涉密档案丢失、被篡改问题时难以及时进行痕迹追

溯。虽然也加强了安全防护建设，但所用的防护设备老化、落后，难以有效抵御新型网络攻击。再加上事业单位发展过程中外部环境复杂多变，涉密档案的流转范围不断扩大，接触人员增多，增加了安全风险发生概率。信息技术的推广应用提升了涉密档案管理效率，但也导致非法获取涉密信息的技术得到升级，增加了涉密档案管理难度，需加强安全防范建设。

### 2.4 人员专业水平待提升

部分事业单位对涉密档案管理的重视度不足，未定期开展保密教育培训工作，工作人员保密意识淡薄，在涉密档案管理中的风险防范不到位，存在随意谈论涉密档案内容、使用非涉密设备处理涉密信息的情况，日常操作中存在违规行为。部分事业单位涉密档案管理人员配置不足，人才队伍建设滞后，工作人员的专业能力待提升，且大多为其他岗位的兼职人员负责涉密档案管理工作，无法保障涉密档案管理的规范性、专业性开展。事业单位还缺乏系统的业务培训和技能考核，档案管理人员难以熟练运用保密技术和信息化工具进行涉密档案的保密管理，增加了泄密风险。

### 2.5 监督考核机制不健全

事业单位涉密档案管理工作开展中，缺乏常态化监督检查机制，日常监督检查主要采用定期抽查方式，检查内容不全面，难以及时排查涉密档案管理中的风险隐患。而且实际检查过程中，主要将重点放在纸质档案和物理环境检查上，忽视对电子档案和网络安全的监督。而且检查过程中各项操作的规范性不足，容易忽视隐性风险。与此同时，部分事业单位未能将涉密档案风险管理纳入绩效考核体系，考核指标不清晰，评价结果与奖惩机制脱节，对违规行为处罚力度不足，制度执行效果差，难以形成有效的约束作用，增加了事业单位涉密档案管理风险的发生率。

## 3 事业单位涉密档案管理风险防控的具体措施

### 3.1 健全涉密档案管理制度体系

事业单位应结合自身职能和涉密档案管理要求，制定专项档案管理制度，确定涉密档案管理办法和相关细则，明确该档案的界定标准、管理流程和操作规范等。细化制度内容，确定秘密等级界定标准、借阅审批流程和存储设备管理要求等，保障专项管理制度的可操作性；健全生命周期管理制度，针对涉密档案各管理环节，制定对应管理内容，例如，在档案收集环节，要确定收集范围、审核标准；在档案销毁环节，要确定销毁方式、审批内容和监督要求等，确保各管理环节都有章可循。

要想筑牢制度防线，则应保证制度内容的有效性，根据国家相关法律法规和档案政策的更新变化，结合信息化发展趋势和事业单位运行发展实际情况，及时更新涉密档案管理制度内容，定期修订、补充与完善，确保制度的时效性、适用性与有效性。除此之外，应保障涉密档案管理制度得到有效执行，严格按照管理职责和管理流程规范操作，做好各环节的风险防范工作，通过有效监督管控，对违反制度的行为进行严肃追责，对保护单位涉密档案有突出贡献的行为进行嘉奖。可将制度执行情况纳入绩效考核体系，以此提高工作人员执行制度的积极性与主动性，保障制度的落实效果。

### 3.2 规范管理流程，加强全生命周期防控

事业单位在涉密档案管理风险防控中，应做好顶层设计，明确涉密档案管理流程和利用标准，对各环节的管理内容进行详细设计。要规范涉密档案形成和收集流程，在档案形成过程中，业务部门安排专人标注秘密等级，确定涉密范围和保密期限，对电子文档进行加密处理；在档案收集环节，档案管理部门应进行严格审核，保证涉密档案的准确性与完整性，细致检查涉密标准是否规范，符合要求的档案应及时归档；在档案利用和借阅环节，需建立严格审批制度，明确审批权限和流程，实现逐级审批。若为绝密档案，需要单位领导审批，明确档案利用范围与使用场所，严禁带出。档案借阅过程中需要详细记录借阅人的信息，要求借阅人不能复制和传播档案内容，如果需要复制则需要办理相关手续。利用电子涉密档案时，则应进行身份认证和权限验证，并利用信息系统记录档案利用痕迹。

涉密档案流转和移交过程中，也要明确具体流程，进行规范作业。采用密封包装、专人护送的方式进行涉密档案流转，并填写流转登记表，确定具体负责人员。向上级部门和协作单位移交涉密档案时，需要审核对方保密资质，签订保密协议，规范交接过程，详细列明移交档案的信息及保密等级，由双方签字确认。涉密档案销毁阶段，需要多部门鉴定确认无价值后再销毁，填写专门的申请表，由负责人员审批。销毁工作需要在指定场所进行，选择适宜的销毁方式，纸质档案采用粉碎方式，电子档案采用消磁或物理销毁方式，整个销毁过程全程监督和录像，销毁后负责人员签字确认，确保档案彻底销毁。

### 3.3 优化存储环境与设备，筑牢物理与技术防线

首先，完善物理存储环境。事业单位需严格按照国家相关标准建设涉密档案库房，应符合“八防”要求，并配备灭火器、除湿机、视频监控、红外报警等设备。要将涉密档案和非涉密档案分开存放，将不同秘密等级的涉密档案分区存储，绝密档案需要单独放置在专门保险柜中。建立库房出入登记制度，严格控制出入人员。其次，加强存储设备管理。应选择符合国家保密标准的档案存储设备，计算机和服务器等硬件设备要设置强密码，对于密码也要定期更换，计算机需安装正版操作系统和杀毒软件，及时升级软件系统和更新补丁。移动存储介质则应安排专人管理，为每个存储介质进行编号，并集中存放，但需要与非涉密存储介质分区存放，禁止交叉使用。在使用之前还需进行安全检测，使用期间定期维修，报废时进行规范处理，以防涉密信息泄露。

对于涉密电子档案，应搭建专门的管理系统，并保证系统功能多元，具备身份认证、访问控制、加密存储和痕迹追溯等核心功能，实现对涉密电子档案的安全管理。在涉密电子档案传输和存储过程中，应进行加密处理，以防涉密信息被窃取、篡改。还要部署防火墙、入侵检测和数据防泄漏系统，加强网络安全设备建设，优化涉密档案网络存储环境，以防遭受黑客攻击和病毒入侵。电子涉密档案管理系统需要定期进行安全检测和风险评估，确保能及时发现安全漏洞并及时修复。另外，还要规范云端存储管理，选择符合国家保密标准的涉密云服务提供商，通过签订保密协议的方式保障涉密档案的安全性。

### 3.4 加强人员管理，提升专业能力素质

涉密档案管理需要政治素养高、责任心强和档案管理专业基础扎实的人员负责，在人才选拔阶段应以上述标准为依据，严格审查待录用人员的综合能力，并签订保密承诺书，明确各岗位人员的保密义务和责任。事业单位应强化保密教育培训，根据风险防控要求，定期开展培训教育活动，培训内容包括保密相关法律法规、涉密档案管理制度、保密技术、风险防控措施等，可采用集中培训、专题讲座、线上学习等方式，增强培训效果，帮助档案管理人员掌握保密知识，在实际工作中实现规范操作。要提升涉密档案管理人员的专业能力，定期开展业务培训，使相关工作人员学习和掌握最新的保密技术与工具，提高涉密档案的保密管理能力。还要为相关工作人员提供行业交流和学习机会，不断提升专业素养和业务能力。事业单位需制定日常行为规范，以此约束涉密档案管理人员的操作行为，明确工作人员禁止操作内容，并通过加强日常监督的方式纠正人员违规行为。

### 3.5 健全监督考核机制，约束档案管理行为

事业单位需建立常态化监督检查机制，成立由多部门负责人员组成的监督检查小组，定期开展涉密档案管理的全面检查工作，保证检查内容覆盖广泛，涉及制度执行、存储环境、设备安全和人员管理等。并采用定期检查与不定期抽查相结合、专项检查与全面检查相结合的方式，确保及时发现隐性风险和管理漏洞。还应加强重点环节监督，严格遵循审查流程和规范标准，同时加强对涉密电子档案系统和网络安全监督，通过审计记录和安全日志及时发现异常操作行为。将涉密档案管理风险防控工作纳入单位绩效考核体系，并将考核结果与奖惩机制相挂钩，表彰奖励表现优秀的部门和个人，考核不合格的需限期整改。还要强化责任追究机制，严格追究违规人员责任，加大处罚力度，以此约束涉密档案管理人员行为。

## 4 结语

事业单位涉密档案管理风险防控工作需要长期、持续开展，面对日益复杂的内外部环境，以及信息技术发展带来的挑战，事业单位应加强涉密档案管理风险防控，完善基础设施，提升档案管理人员的管理水平和风险防控意识，加强制度建设，提供技术支撑，注重全流程风险防控。事业单位也应结合自身实际情况，不断优化风险防控措施，加大技术投入，提高涉密档案管理信息化水平，确保快速适应信息化发展趋势，保障涉密档案管理工作规范、安全、有序开展，有效防范各类风险。

## 参考文献

[1]王雨飞.涉密数字档案管理系统安全保密研究[J].区域治理,2024(16):17-19.

[2]李云兰.事业单位档案信息安全风险及防控策略[J].行政事业资产与财务,2025(4):125-127.

[3]华康民.数字时代涉密档案管理体系框架构建优化研究[J].兰台内外,2024(36):6-8.

[4]马倩,胡亚辰.涉密档案借阅利用存在的问题与对策研究[J].治淮,2024(10):83-84.