涉密文档打印管控方法的探索

张祥坤
中国人民解放军海军勤务学院　天津滨海　300450

摘　要：打印环节作为涉密文档管理的”最后一公里”，在当前高校信息安全防护体系中举足轻重。然而，面对校园设备分散、权限失衡、审计滞后、技术迭代等现实挑战，传统管控方法已难以为继。本文在梳理涉密文档打印管控必要性的基础上，从闭环构建、分级授权、集中管控、系统集成四个方面，探讨了优化高校涉密文档打印管控的实践路径。研究认为，只有坚持”全流程管控、动态精准授权、纵深防御”的原则，并与新兴技术深度融合，才能破解当前管控困局，实现高校涉密文档打印的可管可控、动态平衡。以期为新形势下的高校国防科研安全管理实践提供思路借鉴，助力公办高校筑牢涉密文档安全防线，驾驭数字化转型浪潮。

关键词：涉密文档；打印管控；信息安全；数字化；管控方法

引言

信息时代下，保护涉密文档安全已成为公办高校的重中之重。一方面，《中华人民共和国保守国家秘密法》等法规对涉密信息提出了严格管控要求；另一方面，打印环节因其特殊属性，极易成为泄密的突破口。一旦管控不当，轻则科研成果外泄、学术优势尽失，重则危及国防安全、造成难以弥补的损失。面对高校开放环境与科研保密之间的矛盾，传统的打印管控方法已难以为继。因此，如何从多个维度入手，构建行之有效的涉密级文档打印管控体系，已成为高校国防科研管理中亟待解决的现实课题。

1. 涉密文档打印管控的必要性

1.1 信息安全与泄密防范

在数字化时代，打印作为文档信息载体转换的关键环节，对整个信息安全防护体系至关重要。据《计算机犯罪与安全调查报告》显示，有 85% 以上的安全威胁来自组织内部，其中，最容易忽视的是打印安全，80% 的打印泄密事件几乎都涉及较高等级甚至核心级的商业信息。这一数据警示，打印已成为涉密信息外泄的主要风险点。如果对打印过程缺乏有效监管和必要管控，涉密文档极易经由打印输出这一”最后一公里”，流入非授权人员之手，给组织和个人安全带来难以预估和弥补的损失。因此，从源头遏制打印环节的泄密隐患，建立事前预防、事中监控、事后审计的全流程防控机制，是确保信息安全、守护数据主权的必然要求，也是网络信息时代赋予我们的全新使命。

1.2 涉密保护与竞争优势

对于公办高校而言，核心教材、科研成果、考试试题、学生档案等都是学术建设和人才培养的关键要素，具有极高的保密价值和敏感属性。一旦这些涉密文档在打印环节泄露，很容易被不法分子获取并加以利用，给教学科研带来严重影响。以某高校为例，仅因一名教师将载有期末考试试题的文档打印后被窃取，最终导致考试内容提前泄露和整个评价体系的重大调整 [1]。由此可见，从全流程入手，对涉密文档的打印申请、审批、输出、流转等各个环节进行严密管控，构筑从数字到实体的安全闭环，是维护高校核心学术成果、保障教育教学质量的必由之路，更是摆脱”打印即泄密”的治本之策。

1.3 风险管控与损失预防

涉密文档打印若缺乏规范流程和有效监管，极易引发连锁反应，造成多米诺骨牌效应。譬如，师生随意打印涉密文件，不仅可能触犯《保守国家秘密法》等法律红线，给学院带来严肃问责和声誉受损，更可能引发涉密信息泄露、敏感教学内容外传等一系列衍生风险，给高校人才培养和国防建设带来难以预计的损失。为了防患于未然，亟需将打印环节纳入全局风险管控视野，建立从涉密资料分级、教职员工权限、行为审计到应急处置的一体化防控体系。通过事前风险预警、事中行为监管、事后全面审计，最大限度降低涉密信息泄露概率，将潜在安全隐患控制在可接受范围，做到心中有数、管控有方。

2. 涉密文档打印管控的现实挑战

2.1 设备分散与监控困难

在当前高校信息化建设中，打印机作为常见的外设，其管理模式大多还停留在各院系自行采购、自主管理的粗放状态。这种分散式的管理方式，虽在一定程度上提升了各院系打印的灵活性和便捷性，但对涉密文档的打印监管却埋下了诸多隐患。由于缺乏信息中心在线集中监控的技术手段，管理者难以实时掌握各教学单位打印设备的使用状态，对哪些师生打印了哪些涉密教材更是一无所知。而分散在各处的纸质打印审计记录，其完整性和准确性也无从保证，一旦出现涉密资料泄密事件，想要第一时间锁定打印源头更是难上加难 [2]。此外，随着线上教学、校外实践等新场景的涌现，学院对外延伸的打印边界愈发模糊，使得设备管控的盲区进一步扩大。这种基于特定场所的静态管理思路，面对日益开放、多元化的高校打印行为，其固有缺陷日益凸显，亟需引入创新的管理理念和技术手段，重构高效协同、动态感知的集中监管格局。

2.2 权限细化与效率冲突

不少高校虽已意识到精细化权限管控的必要性，但受制于技术手段滞后、管理流程僵化等现实因素，往往难以真正落到实处。理想的权限模型要求从教职人员身份、涉密资料密级、教学场景等多个维度，对涉密打印行为进行细粒度管控。比如针对密级教材，应从源头严控打印权限，遵循最小化原则，审批流程须由院领导逐级把关；而一般教学资料则可相对放宽限制，但须明确使用范围等。然而，在现实中推行如此细化的权限体系，势必会带来诸多副作用。过于繁琐的审批环节无疑会延长打印等待时间，像临时教学备课、紧急授课需求等常态化需求更难以满足，实际教学效率必然大打折扣。而师生对管控措施的心理抵触也会相应增大，不利于提升整体安全意识。由此可见，在制度设计和执行层面，如何权衡涉密资料精细管控与教学打印效率之间的矛盾冲突，是一个长期困扰高校管理者的现实难题。

2.3 审计滞后与追溯不力

事后审计在涉密级文档打印管控体系中举足轻重，是确保合规性、及时止损的关键一环。然而，不少高校的审计流程和技术方案却难以适应信息保密的严格要求。首先，传统的打印日志大多只记录表面元数据如文件名、页数、时间等，缺乏对教材内容的实时解析和风险判定。这就造成保密管理者只能做”马后炮”，而无法精准感知异常打印行为、及时阻断违规操作。其次，在已发生的涉密资料泄密事故中，由于缺乏长期、完整的教学资料打印记录，事后的责任追溯也往往流于形式 [3]。特别是面对校外人员的蓄意窃密，单靠表面线索往往难以厘清责任主体、实施有效问责。

2.4 技术迭代与漏洞增加

技术创新固然是高校信息化建设的助推器，但其带来的负面影响同样不容忽视。譬如，智能打印、云打印等新技术在带来便利的同时，也引入了新的风险变量。一方面，涉密教材打印介质从传统纸张向多样化载体的延伸，大大拓宽了涉密信息的传播途径，使得传统的监管手段难以全面覆盖。另一方面，校园网络基础设施的升级虽提升了教学科研效率，但也不可避免地引入了涉密数据泄露、未授权访问等新的安全隐患。而开放式打印系统的普及，更是直接将高校内部的涉密教学资源暴露在了潜在攻击者面前。面对日新月异的技术场景，传统的事后封堵思路已难以为继，必须转变理念，从动态感知、主动免疫的角度构筑纵深防御体系。与此同时，校园内各类打印设备自身的脆弱性也须高度关注。随着设备固件版本、驱动程序的频繁迭代，潜在的系统漏洞层出不穷。

3. 涉密文档打印管控的优化路径

3.1 闭环构建与全程监管

针对涉密文档打印的特殊性，单点式的管控方法已难以满足高校实际需求。我们必须立足全局，从端到端构建起一套闭环式的安全防护体系。具体而言，事前阶段要充分发挥涉密资料密级标识和访问控制的作用，采用透明加密技术对拟打印的涉密教材进行自动加密，并基于教职人员岗位设置差异化的打印权限，对于高密级教学文档须通过院系逐级审批方可打印，从源头防范泄密风险；事中阶段则要全方位记录打印全过程数据，包括资料内容、教师身份、设备指纹等关键要素，运用智能算法审核打印行为的合规性，一旦发现异常可自动阻断打印；事后阶段还要在纸质教材中植入隐形水印，借助文档溯源技术快速定位打印人和设备，并对废弃涉密资料进行集中回收和安全销毁。如此形成的事前、事中、事后全流程管控闭环，方能最大限度消减涉密资料打印的泄密风险。唯有构建起事前预警、事中监管、事后审计的端到端防护链条，将教学人员、设备、介质、环境等要素全方位纳入管控视野，通过制度规范和技术手段的有机结合，

持续优化动态防御能力，才能真正实现对涉密文档打印的风险感知、主动发现和精准阻断 [4]。

3.2 分级授权与动态审批

在涉密文档打印管理中，如果对所有教材和师生都采取”一刀切”的授权策略，要么会影响教学效率，要么会留下安全死角。因此，构建一套灵活的分级授权机制至关重要。根据教材的密级程度进行科学分类，对于绝密级资料，打印权限应严格限定在最小教师范围内，并缩短授权有效期，而对于机密级以下教学资料则可适度放宽限制，但仍需明确教学场景和使用范围。与此同时，针对临时性、突发性的教学打印需求，还应建立一套动态申请与审批流程，教职员工可按需发起一次性授权申请，在获得相应级别院领导的审批许可后方可打印，且该授权在使用后立即失效。这种将”盖棺定论式”的静态授权与”按需申请式”的动态授权相结合的模式，既可在确保秘密安全的前提下满足灵活教学的需要，也能最大程度降低因常态化授权而引发的资料泄密隐患。分级授权是平衡教学效率与安全的有效之举，而动态审批则为特殊教学场景下的弹性授权提供了现实路径。

3.3 集中管控与销毁机制

在高校教育领域或针对特定资料，物理隔离和集中管控仍不失为一种行之有效的管理方法。对于教材等核心机密，可划定独立的教学资料打印场所，配备专属打印设备和监控设施，从物理和网络两个层面与校园网进行隔离。同时，应从制度层面明确规定教材打印人员和设备的准入门槛，严防无关师生接触涉密文件。对于打印输出的教材，还须细化介质全生命周期管理流程，确保从领用到课堂使用再到销毁的全过程可管可控、可审可溯。针对废弃教材，要采用物理粉碎和化学溶解等手段进行彻底销毁，且全程录像存档备查，坚决杜绝二次泄密的风险。应看到，在某些极端场景下，投入大量人力物力开展集中管控虽不便教学协同，但对于守护关乎国防安全的机密不可或缺。集中式的涉密资料打印管理模式，虽然在一定程度上会增加使用不便，影响教学效率，但安全至上始终是底线原则。随着安全形势的不断变化，我们还需与时俱进地优化集中管控的实施路径，在最小化影响教学连续性的同时，持续强化隔离防护、访问控制、销毁审计等关键环节，筑牢涉密信息的安全防线。

3.4 系统集成与智能升级

随着教育信息化的日新月异，传统的单一管控手段已难以全面覆盖高校日益复杂的涉密资料打印场景。为了真正做到涉密教材打印无死角、管控无盲区，必须审时度势，主动拥抱前沿科技成果，推动系统集成和能力升级。一方面，应立足全院视角，在现有教师身份认证、权限管理、行为审计等基础上，将涉密打印管理系统与校园信息系统有机整合、互联互通，形成统一的安全管控平台，确保教职工账号、授权策略、操作日志等数据的实时共享和自动校验；另一方面，还应积极引入人工智能、大数据分析、教学流程自动化等新兴技术，通过动态构建教师画像、智能分析异常打印行为等方式，实时发现潜在威胁，并依托软件定义安全动态调整防护策略，最终形成一套自适应、自进化的智慧防护体系 [5]。可以预见，随着新技术与资料打印管控的深度融合，传统静态管控必将让位于泛在智能防护，成为新时期密级文档安全的必由之路。这是顺应高校信息化、数字化发展大势，实现涉密资料打印智慧升级，构建纵深防御体系的必然选择。

4. 结束语

涉密文档打印是高校信息安全管理中的重要一环，直接关系到人才培养教材能否安然无恙。面对新形势下的管控挑战，既要坚持”全流程管控、多层次防护、动态精准授权、集约高效利用”的基本原则，更要与时俱进地拥抱人工智能、大数据等新技术，用系统化的思维打造纵深防御体系。唯有在制度规范、技术手段、师生意识等方面形成合力，才能有效遏制打印环节的泄密风险，为高校教育乃至国防安全保驾护航。站在教育数字化转型的风口，涉密文档打印管控理应担负起院校安全赋予的新使命。

参考文献：

[1] 纪东营 . 档案信息保密的重要性研究 [C]// 中国智慧工程研究会智能学习与创新研究工作委员会 .2022 社会发展论坛（昆明论坛）论文集 . 中国石化集团共享服务有限公司东营分公司 ;,2022:93-98.

[2] 董秦刚 , 范力思 . 涉密电子文档管理中需要注意的安全因素 [J]. 计算机产品与流通 ,2019,(02):93.

[3] 汤蕊 , 梁绍翔 , 朱海波 , 等 . 创新打印模式实现文档生命周期闭环管理 [J]. 保密科学技术 ,2017,(09):60-62.

[4] 苏宾 , 杨艳国 , 成立权 , 等 . 军工企业涉密文档打印管理的创新与实践 [J]. 中国管理信息化 ,2014,17(20):79-81.

[5] 苏宾 . 涉密文档打印管控方法的探索与实践 [J]. 黑龙江科学 ,2014,5(09):186.