聚知刊出版社
JZK publishing

新时代办公室公文处理中的保密风险防控机制研究

林彦彤

福建华电可门发电有限公司，福建省福州市，350000；

摘要：在新时代数字化办公与国企改革深度融合的背景下，办公室作为企业信息流转的核心枢纽，其公文处理工作既承担着政策传达、决策支撑的关键职能，也面临着涉密信息泄露的多重风险。本文以某电厂办公室公文处理实践为研究对象，结合其在保密管理、公文流转、系统运维等方面的制度设计与执行经验，系统梳理公文处理全流程中存在的保密风险点，包括载体管理不规范、人员意识薄弱、技术防护不足、流程管控漏洞等问题。在此基础上，从制度完善、人员管理、技术升级、流程优化四个维度，构建“人防+技防+制防”三位一体的保密风险防控机制，旨在为同类企业提升公文处理保密工作水平、保障国家秘密与商业秘密安全提供实践参考。

关键词：新时代公文处理保密风险防控机制

DOI：10.69979/3029-2700.26.01.087

引言

公文作为企业履行职能、传递信息、规范管理的重要载体，其处理质量直接关系到决策效率与执行效果。而在能源、电力等关系国计民生的重点行业，公文中常涉及国家秘密、商业秘密及内部敏感信息，保密工作更是公文处理的生命线。随着办公自动化（OA）系统的普及、电子公文的广泛应用，以及外部环境中网络攻击、信息窃取手段的多样化，办公室公文处理面临的保密风险日益复杂——既有传统纸质载体管理不当导致的泄露风险，也有电子公文在传输、存储、归档过程中的技术安全隐患，还有人员保密意识薄弱引发的操作失误风险。

某电厂作为能源领域的重要企业，其办公室公文处理涵盖党委文件、行政文件、涉密会议纪要、商业秘密材料等多种类型，涉及定密管理、载体流转、人员管控、系统运维等多个环节。近年来，该电厂通过制定《保密工作管理细则》《公文处理办法》《OA 系统使用管理细则》等制度，在公文处理保密工作中积累了一定经验，但仍面临数字化转型带来的新挑战。因此，以该电厂为研究样本，深入分析公文处理全流程的保密风险，构建科学有效的防控机制，不仅对该电厂自身安全发展具有重要意义，也能为同类企业提供可借鉴的实践路径。

1 某电厂办公室公文处理中的保密风险点梳理

公文处理是一个包含“拟制—审核—签发—流转—归档—销毁”的全流程闭环，每个环节均存在潜在的保密风险。结合某电厂公文处理实践，其保密风险主要集中在以下四个维度：

1.1 载体管理维度：纸质与电子载体双重风险叠加

公文载体分纸质（如涉密文件等）与电子（如涉密 U 盘等）两类，其管理漏洞是保密风险主因。纸质载体存在“全流程管控不严”问题。某电厂《保密工作管理细则》要求涉密纸质文件“全程闭环管理”，如机密级 2 日内、秘密级 3 日内归还并存放专用柜，但实际部分部门存在“逾期未归”“随意存放”现象，扩大涉密信息接触范围；尤其在销毁环节，涉密材料草稿、过程稿未按涉密文件管理要求销毁，存在私自用非涉密碎纸机处理或随意丢弃的情况，增加信息泄露风险。电子载体存在“技术防护不到位”问题。某电厂规定涉密电子文件在专用计算机处理，严禁连互联网及非涉密设备；同时，OA 系统虽设置权限管理功能，但部分用户存在“密码长期不换”“账号转借”的违规行为，导致电子公文被非授权访问。

1.2 人员管理维度：保密意识与专业能力不足

人员是公文处理保密工作核心主体，其保密意识和专业能力直接决定风险防控效果。某电厂人员管理存在两类突出问题：一是保密意识薄弱，“习惯性违规”频发。部分员工对保密工作重要性认识不足，视“保密规定”为“形式要求”，如公开场合讨论涉密公文细节；部分员工在新闻宣传、信息公开工作中，未经相关流程审批直接发布内容，导致敏感信息泄露；涉密会议未严格执行设备管理要求，未将手机放置手机屏蔽柜且未加装信号屏蔽器，存在信息外泄隐患；新入职员工未接受系统保密培训就参与公文处理，不了解涉密文件识别标准与管理流程，易因“无知”失误。二是专业能力不足，“操作不规范”问题突出。公文处理定密、分密、解密等环节需专业知识，但部分员工缺乏相关能力，如拟制

公文时未按规定填写《国家秘密确定审批单》、误标密级，涉密人员离岗未按流程办理清退和脱密期管理手续。

1.3 流程管控维度：关键环节存在漏洞

公文处理流程的审核、流转、归档等关键环节，缺乏严格管控易成保密风险“突破口”。某电厂流程管控存在三方面漏洞：审核“形式化”，未发挥“把关”作用。制度要求公文签发前办公室审核，检查密级标注等内容，但实际部分审核人员只关注格式，忽视内容涉密性，如未发现未脱敏商业数据、未审核附件涉密信息，导致“涉密附件随非涉密公文流转”。流转“跟踪难”，责任追溯不清。电厂规定涉密公文专人传递并记录轨迹，但部分部门为省时让非涉密人员传文件、不及时记录；电子公文流转无“实时提醒”，文件滞留无法督促处理，增加泄露风险。归档“管理乱”，涉密与非涉密文件混放。电厂要求涉密公文单独存放并标注密级期限，但部门经办人员不清楚相关文件需按派生定密定位工作秘密，未进行定密后将文件作为附件，随非涉密文件归档。

1.4 技术支撑维度：数字化转型带来新挑战

随着某电厂推进“数字化办公”，应用 OA 系统、数字档案馆等技术平台，虽提升公文处理效率，但带来新保密风险：一是 OA 系统有“安全漏洞”。它是电子公文流转核心平台，权限设置“一刀切”，未按“最小必要原则”细化，且缺乏“异常行为监测”功能，难以及时发现风险操作。二是数字档案馆“防护不足”。该馆存储大量商密文件和内部信息，未用加密存储技术，仅靠简单认证方式，且档案备份机制不完善，遇网络攻击或硬件故障，可能导致数据丢失和商密信息与内部敏感信息被窃。三是移动办公“风险失控”。部分员工用移动设备访问 OA 系统处理公文，设备缺保密防护软件，易被植入恶意程序，且丢失或被盗时无“远程擦除”功能，会造成涉密文件泄露。

2 某电厂办公室公文处理保密风险防控机制构建

针对上述风险点，结合某电厂的制度基础与实践需求，应构建“制度完善—人员提能—技术升级—流程优化”四位一体的保密风险防控机制，实现“人防、技防、制防”的深度融合。

2.1 完善制度体系，筑牢“制防”基础

制度是保密风险防控的“根本遵循”，需在现有制度框架下，进一步细化规定、填补漏洞，形成“覆盖全流程、责任全明确”的制度体系。

制定《公文处理保密风险管控细则》，明确各环节责任。在现有《保密工作管理细则》《公文处理办法》基础上，新增专项细则，对公文拟制、审核、流转、归档、销毁等环节的保密要求进行细化：例如，在拟制环节，明确“谁拟稿、谁负责”，要求拟稿人必须填写《涉密文件审核表》，经部门负责人、保密办双重审核后方可上报；在流转环节，规定“涉密公文必须由机要人员传递，且需全程携带保密包，传递轨迹实时记录”；在销毁环节，建立“双人清点、双人押运、双人监销”制度，销毁后需填写《销毁涉密载体确认表》，由监销人签字存档。

完善《涉密人员管理办法》，强化全周期管控。针对涉密人员意识薄弱、能力不足的问题，细化管理要求：一是严把“入口关”，新入职涉密人员需通过保密知识考试、背景审查后方可上岗，并签订《涉密人员保密承诺书》；二是加强“日常管理”，要求涉密人员每年接受不少于 8 学时的保密培训（原规定为 4 学时），培训内容涵盖最新保密法规、典型案例、技术防护技能等；三是严控“出口关”，涉密人员离岗时，需办理“涉密载体清退—脱密期审批—保密提醒谈话”手续，脱密期内由人力资源部与保密办联合跟踪，定期开展回访。

制定《数字化办公保密管理规定》，应对技术风险。针对 OA 系统、数字档案馆、移动办公的风险，明确技术防护要求：例如，OA 系统需设置“分级权限”，根据岗位职能细化访问权限（如普通员工仅可查看非涉密公文，部门负责人可查看本部门涉密公文）；数字档案馆需采用“加密存储+双备份”技术，备份数据分别存放于本地与异地，防止数据丢失；移动办公需使用公司统一配发的保密手机，安装防泄密软件，禁止通过非授权软件传输公文。

2.2 强化人员提能，夯实“人防”核心

人员是保密风险防控的“第一防线”，需通过“培训+考核+激励”相结合的方式，提升员工的保密意识与专业能力。

构建“分层分类”培训体系，提升专业能力。针对不同岗位、不同层级的员工，设计差异化培训内容：一是“全员普及培训”，每年组织 1 次全员保密知识考试，内容包括保密法规、公文保密标准等，考试不合格者需补考；二是“专项技能培训”，对拟稿人、审核人、机要人员等关键岗位员工，开展“公文定密技巧”“涉密载体管理”“OA 系统安全操作”等专项培训，邀请保密局专家现场授课；三是“应急演练培训”，每半年组织 1 次保密应急演练，模拟“涉密文件丢失”“电子公文被窃取”等场景，提升员工应急处置能力。

建立“量化考核”机制，压实保密责任。将保密工作纳入员工绩效考核，制定《公文处理保密考核细则》：例如，若员工出现“涉密文件逾期未归”“账号转借他人”等违规行为，每次扣减绩效分 5 分，并取消年度评优资格；若因个人失误导致涉密信息泄露，除考核外，还需承担相应责任（如通报批评、降职）；反之，若员工在保密工作中表现突出（如及时发现风险隐患、提出有效改进建议），给予绩效奖励（如每次奖励 100-300 元）。

加强“文化建设”，营造保密氛围。通过多种形式提升全员保密意识：一是定期发布“保密警示”，在 OA 系统首页、公司公告栏发布典型泄密案例，提醒员工警惕风险；二是开展“保密月”活动，每年 9 月组织“保密知识竞赛”“保密主题演讲”等活动，增强员工参与感；三是设置“保密监督员”，在各部门选拔 1 名责任心强的员工担任兼职保密监督员，负责日常监督本部门公文处理的保密情况，发现问题及时上报。

2.3 升级技术防护，强化“技防”支撑

技术是保密风险防控的“重要手段”，需引入先进技术、优化现有系统，构建“全方位、智能化”技术防护体系。

首先，优化 OA 系统安全功能，实现“智能管控”。联合生产技术部升级 OA 系统，一是增加“异常行为监测”模块，实时监测用户登录地址与操作行为，发现异常自动锁定账号并向保密办预警；二是设置“公文流转提醒”功能，对滞留超 24 小时的公文，自动向经办人、部门负责人短信提醒；三是添加“水印防伪”功能，商密文件下载时自动生成含用户姓名、下载时间的水印，且水印不可复制张贴，禁止使用未安装商密打印机打印。

其次，升级数字档案馆防护能力，保障“数据安全”。对数字档案馆技术改造，一是设置“多因素认证”，访问档案需“用户名+密码+动态口令”三重验证；二是建立“实时备份”机制，档案数据每小时自动备份 1 次，备份数据存于加密服务器，进一步保障商密文件和内部信息存储安全。

最后，推广“保密办公设备”，降低移动办公风险。为涉密人员配备专用保密设备，一是配备采用硬件加密技术的“涉密 U 盘”，仅可在专用涉密计算机使用，接入非涉密设备自动锁定；二是在保密要害部位安装“手机信号屏蔽器”，防止员工在涉密场所拍照、传输信息。

2.4 优化处理流程，实现“全周期”管控

流程是保密风险防控的“关键环节”，需重构、强化监督，确保公文处理全流程“可追溯、可管控”。

重构审核流程，强化“双重把关”。将原“办公室单一审核”改为“部门初审+办公室复审+保密办终审”三级审核流程：部门负责人初审公文涉密性，公文管理员复审密级标注与格式规范，保密办主任终审是否合规及有无遗漏风险。三级审核均填《公文保密审核记录表》，签字存档，实现“谁审核、谁负责”。

优化流转流程，实现“全程追溯”。针对纸质公文流转“跟踪难”，建立“涉密公文流转电子台账”，实时记录文件传递、接收人员及时间等信息，由保密办动态监控，一旦出现逾期未流转情况自动预警，确保责任可追溯。

规范归档流程，实现“分类管理”。针对归档“混放”问题，制定《公文归档保密管理规范》：明确“分类存放”，涉密公文存保密档案柜，采用“双人双锁”；建立“档案借阅审批”制度，借阅需填单经双重审批，在保密室查阅；每季度开展“档案保密检查”，清查风险。

3 结论与展望

办公室公文处理保密风险防控是新时代国企安全管理重要部分，也是企业高质量发展关键支撑。本文以某电厂为对象，梳理其公文处理中载体、人员、流程、技术四类风险点，构建“制度完善—人员提能—技术升级—流程优化”防控机制，为同类企业提供参考。该机制有效落地可实现三个“提升”：一是通过制度细化与技术监测提升保密风险“预判能力”，提前发现潜在风险；二是通过人员培训与应急演练提升风险处置“响应能力”，确保快速处置；三是通过考核激励与文化建设提升保密管理“长效能力”，形成良好氛围。随着数字化发展，公文处理保密风险更隐蔽复杂，如人工智能可能破解保密系统、量子计算威胁加密技术等。因此，企业要持续关注技术趋势，更新防控手段，加强与同行交流合作，共享经验，构建“安全、高效、智能”保密管理体系。

参考文献

[1]刘月梅.Y 区党政机关公文处理流程数字化再造问题研究[D].中共山东省委党校,2023.
[2]伏强.中国电子行政审批系统运行保障体系问题研究[D].吉林大学[2025-09-16].DOI:CNKI:CDMD:2.1017.140080.
[3]郑丽娜.基于沙箱防护技术的OA管控系统的设计与实现[D].重庆大学,2014.