

档案软件 - 档案访问日志记录功能【云丰档案软件功能介绍】

档案管理软件 · 安全管理功能介绍

具体谁查阅、下载了哪一份档案，应当单独记录。云丰档案对档案的访问行为专门记日志：把阅览、下载、复制等针对具体档案的动作与人、档号、时间对应起来，形成档案维度的访问记录，敏感档案被谁动过一查便知。

一、为什么需要档案访问日志记录

操作日志记的是做了什么，访问日志记的是碰了哪份档案，这对档案管理尤为关键：

动档无据：谁调阅了哪份敏感档案，查不到；

敏感失控：涉密档案被不适当访问却没有记录；

事后难核：出了泄密，无法排查谁接触过该档；

利用无统计：哪些档案被频繁访问，缺乏数据支撑。

访问日志要把人和具体档案对应起来：哪份档案被谁看过下过，记得清清楚楚。

二、怎么用

用户阅览、下载档案时，系统记录该次访问并关联档号与访问人：

表1 档案访问日志记录内容

记录项	说明
访问人	记录查阅或下载档案的人员
访问对象	关联所访问档案的档号与题名
访问方式	区分在线阅览、下载、复制等
访问时间	记录访问发生的时间
按档检索	可按档案反查其访问历史

访问日志与操作日志互为补充：操作日志面向功能动作，访问日志面向档案对象。管理员既能按人查访问了哪些档，也能按档查被哪些人访问过。

谁、在何时、以何种方式查阅或下载了哪份档案，逐件记录在案；敏感档案的每次访问都可回溯到具体人。日志与档案挂接，调出案卷即可看到其访问史。

日志与案卷挂接，调出任一案卷即可看到其访问史；敏感档案被谁、何时、以何方式看过逐件可溯。一旦发生外泄，可据日志快速划定查看范围、追溯泄露环节，让每一次调档都留下姓名，守住利用可追溯的底线。

日志按密级与敏感件重点标注，安全检查时可直接调出某份涉密档案的访问史，快速判断是否存在异常调阅。

调出任一案卷即可看到其访问史，敏感件被谁看过全程透明，外泄时可据以追溯。

日志与案卷、借阅记录相互印证，既看到谁看过，也看到为何看。

每次预览、下载、打印都留下记录，调阅行为可回溯，为泄密事件提供取证依据。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
人档对应	谁动过哪档	访问人与具体档案档号关联记录。
按档反查	这档谁看过	可反查某份档案的全部访问历史。
方式细分	阅览下载分开	区分在线看、下载、复制等动作。
敏感监控	重点关注	敏感档案访问单独可查可控。
利用分析	热门有数	为利用统计与开放鉴定提供数据。

它让涉密档案被谁看过全程透明，一旦外泄可据日志追溯泄露范围。

四、典型使用场景

- 泄密排查：档案外流时按访问日志锁定接触人；
- 敏感监控：关注涉密档案被谁访问过；
- 利用统计：按访问频次分析档案利用情况。

五、价值与产品定位

档案访问日志把人和具体档案精确对应：谁在何时看了、下了哪份档案，记录完整。一旦出现泄露或争议，能按档反查接触过的人，也为利用统计和敏感监控提供了数据基础。它让每一次调档都留下姓名。

它与操作日志、登录日志形成立体审计：登录入口、系统操作、档案访问各有记录。云丰档案借此让敏感档案的每一次接触都留痕，支撑密级管控和合规审计。云丰档案以访问日志守住档案利用的可追溯底线。