

档案软件 - 安全性检测功能【云丰档案软件功能介绍】

档案管理软件 · 功能介绍

进馆文件可能携带病毒或恶意代码，一旦感染档案库将波及全部数据。云丰档案的安全性检测功能在归档入口自动查杀病毒、扫描恶意代码，并检查敏感信息与开放风险，把安全隐患拦截在档案库之外。

一、为什么需要安全性检测

档案库是单位数据的集中地，安全防线必须设在入口：

病毒带入：外来文件带毒上传，感染后波及整个档案存储；

恶意代码：夹带宏病毒、脚本的文件在利用时触发风险；

敏感泄露：归档文件中含不应公开的敏感信息却未被发现；

外发失控：缺乏安全检查，档案对外提供时带来泄露风险。

安全性检测要解决的是文件带不带毒、藏没藏恶意代码、有没有敏感信息这三件事，守住档案库的安全入口。

二、怎么用

文件上传归档时，系统自动进行病毒查杀与安全扫描，发现风险即拦截并提示：

表1 安全性检测内容

检测项	检测内容
病毒查杀	自动扫描文件病毒、木马与恶意程序
恶意代码	检查宏、脚本等可执行内容的安全风险
敏感信息	识别文件中不应公开的敏感数据
开放风险	检查外部链接、嵌入式对象等潜在风险
拦截处置	发现风险文件阻止入库并提示处理

带毒文件一律拦截上传，待清除风险后再归档。检出敏感信息的文件进入脱敏或保密审查流程，不得直接公开。在实际使用中，档案员可以结合本单位的安全性检测工作习惯，在不改变整体流程的前提下微调各环节的先后顺序；系统会自动记录每一步的操作人、操作时间与处理结果，使安全性检测全过程留痕可

溯，事后复盘或接受审计时都能还原当时情形，不必担心操作无据可查。在权限安排上，与安全性检测相关的操作按三员分离原则分级授权，业务经办人、档案管理员与系统管理员各司其职，越权操作会被系统自动拦截；这一机制让安全性检测既能高效流转，又始终处于受控状态，避免权限集中带来的风险。云丰档案在设计安全性检测时充分考虑了不同单位的差异，相关规则、字段与流程均可按本单位实际配置，并不强求千篇一律；配合多格式上传、病毒扫描、OCR 识别与 AI 分类等通用能力，安全性检测与整套档案管理流程自然衔接。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
病毒查杀	入口即防线	上传自动查杀，带毒文件不入库，保护档案库整体安全。
恶意代码扫描	风险早发现	检测宏、脚本等，防止利用时触发安全事件。
敏感识别	泄露可预防	识别文件中敏感信息，转入脱敏或保密流程。
拦截留痕	处置可追溯	风险文件拦截记录留存，问题可追查。
持续更新	库源及时	病毒库与规则持续更新，应对新型威胁。

四、典型使用场景

- 外部文件归档：外来移交文件先查杀后入库，防止带入病毒；
- 敏感归档：归档时识别敏感信息，触发保密审查；
- 对外提供：外发文件前做安全与敏感检查，防止泄露。

五、价值与产品定位

安全性检测的价值，是给档案库装上安全门：带毒的进不来，藏害的早发现，敏感的先审查，集中存放的数据才有安全保障。

它是四性检测的安全一环，与脱敏、保密审查、权限分级协同。云丰档案以三员分离、加密存储和信创适配构建纵深安全防护。从长期运行看，安全性检测产生的数据会持续沉淀在档案库中，随日常利用不断积累丰富；系统支持按时间、部门、类别等维度统计与导出，可定期形成安全性检测运行情况的汇总，为管理决策和迎检备查提供扎实的数据支撑，而不是一笔糊涂账。对于已经积累了

大量历史档案的单位，安全性检测相关的管理经验可以逐步迁移到本功能上来，不必一次性推倒重来；单位可以边使用边优化规则与流程，让安全性检测逐步贴合自身的管理要求，降低推行阻力。