

档案软件 - 敏感数据脱敏功能【云丰档案软件功能介绍】

档案管理软件 · 功能介绍

档案利用中常需对外提供，但身份证号、手机号、金额等敏感信息不能原样暴露。云丰档案的敏感数据脱敏功能按规则对档案中的敏感字段自动变形，在保留档案可用性的同时保护个人隐私与商业秘密。

一、为什么需要敏感数据脱敏

档案对外提供与信息保护之间存在天然张力：

原样外泄：整份档案对外提供，敏感个人信息一并暴露；

手工打码：人工遮挡敏感信息费时费力，还容易漏挡；

影响利用：为保密把档案封死，合理利用也无法开展；

规则不清：哪些字段该脱敏、怎么脱敏没有统一标准。

脱敏要解决的是敏感信息不外露、档案还能用、脱敏规则统一这三件事。

二、怎么用

对外提供档案时，系统按预设脱敏规则自动对身份证号、手机号等敏感字段变形，输出脱敏版本：

表1 敏感数据脱敏流程

环节	操作要点
识别敏感项	自动识别身份证、手机号、银行卡等敏感字段
套用规则	按字段类型套用掩码、替换等脱敏规则
生成脱敏版	输出敏感信息变形、其余内容完整的版本
水印标记	脱敏件加水印与用途标记
原始受控	原件仍按密级严格管理，不随意外发

授权用户看到脱敏版本，确需完整信息的走单独审批。脱敏过程留痕，对外提供的都是处理后的安全版本。在实际使用中，档案员可以结合本单位的敏感数据脱敏工作习惯，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，使敏感数据脱敏全过程留痕可溯，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，与敏感数据脱敏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；这一机制让敏感数据脱敏既能高效流转，又始终处于受控状态，避免权限集中带来的风险。云丰档案在设计敏感数据脱敏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，敏感数据脱敏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
自动识别	敏感项不漏	自动识别常见敏感字段，不必人工逐个找。
规则脱敏	变形不暴露	按字段掩码或替换，既保护隐私又保留可读性。
脱敏输出	对外安全	对外提供脱敏版本，原件不外泄。
水印留痕	外流可追	脱敏件加水印与用途，流出可追踪责任。
分级授权	需全量再审批	确需完整信息走单独审批，平衡利用与保护。

四、典型使用场景

- 对外公开：档案开放利用时输出脱敏版本供公众查阅；
- 合作共享：与外部机构共享档案时屏蔽敏感个人信息；
- 研究使用：科研利用时提供脱敏数据，保护当事人隐私。

五、价值与产品定位

敏感数据脱敏的价值，是让档案既能用又不泄密：敏感信息变了形，隐私和商业秘密不露，合理利用照常进行。

它与保密审查、权限分级、安全检测协同，构建档案信息保护体系。云丰档案以三员分离、加密存储和信创适配满足数据合规要求。从长期运行看，敏感数据脱敏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，可定期形成敏感数据脱敏运行情况的汇总，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，敏感数据脱敏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，让敏感数据脱敏逐步贴合自身的管理要求，降低推行阻力。