

档案软件 - 档案数据加密存储功能【云丰档案软件功能介绍】

档案管理软件 · 功能介绍

档案里有大量敏感信息，存储时不能是明文。档案数据加密存储对入库电子文件加密后再落盘，即使存储介质被盗，没有授权也无法读取内容，守住数据安全。

一、为什么需要档案数据加密存储

档案数据一旦泄露后果严重，但很多系统只是把文件明文凭在磁盘上：

明文落盘：文件未经加密直接存在磁盘上，拷走即可打开。

介质失窃风险：硬盘、存储设备一旦丢失或被盗，数据立刻外泄。

越权拷贝：有人能直接访问存储目录，绕过系统把文件拷走。

合规要求：敏感档案明文存储不满足数据安全合规要求。

加密存储要让文件“落地即加密”：数据以密文形态存放，只有通过授权和密钥才能解密阅读。

二、怎么用

文件入库时系统自动加密后存储。主要环节如下：

表1 档案数据加密存储流程

环节	系统处理说明
入库加密	文件通过校验后，系统自动加密再写入存储
密文落盘	磁盘上保存的是密文，不是可直接打开的明文
授权访问	用户通过系统调阅时，按权限在线解密展示
密钥管理	密钥由系统统一安全管理，与数据分离
全程受控	下载、打印等操作按权限控制并留痕

加密对正常使用透明：授权用户在系统内调阅照样打开。但脱离系统直接拷贝存储文件，拿到的只是无法读取的密文。文件入库即加密后落盘，磁盘上保存的是密文。授权用户在系统内调阅时按权限在线解密，体验不受影响；脱离系统直接拷贝存储文件，得到的只是无法读取的密文。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
落地加密	文件密文存盘	入库自动加密，磁盘上是密文，拷走也读不出内容。
授权解密	用着不影响	通过系统按权限在线解密，正常调阅体验不变。
密钥分管	安全有保障	密钥与数据分离管理，避免单点泄露风险。
介质防护	失窃不泄露	存储设备丢失被盗，数据仍以密文形态安全无虞。
合规存储	满足要求	加密存储符合敏感数据保护与档案安全合规要求。
密钥分管	安全可控	密钥与数据分离管理，避免单点泄露风险。

四、典型使用场景

- 涉密档案保管：涉密文件加密存储，介质失窃也无法被读取。
- 敏感数据防护：人事、财务等敏感档案加密落盘，防止越权拷贝外泄。
- 合规存档：按数据安全要求对归档文件加密，满足监管检查。

五、价值与产品定位

加密存储给档案数据加了一道“落地锁”：文件以密文存放，介质被盗也读不出，授权使用却不受影响，数据安全与合规双达标。加密存储给档案数据上了一道落地锁，介质被盗也读不出，是敏感档案安全合规的底线要求。静态加密是数据安全的基本要求：文件一旦落盘，就应当以密文形态存在。这样即使存储介质流失，没有密钥也无法还原内容。授权用户在系统内的正常调阅却不受影响，安全与便利由此兼得。

它是云丰档案存储安全体系的基石，与权限三员分离、完整性校验、异地备份协同，保障档案在存储、传输、利用各环节全程可控。档案里沉淀着大量敏感信息，一旦存储介质丢失或被绕过系统直接拷贝，明文文件就会外泄。入库即加密、磁盘只存密文，配合密钥分管和授权在线解密，让数据在静态存储时始终受到保护。