

档案软件 - 备份数据加密功能【云丰档案软件功能介绍】

档案管理软件 · 功能介绍

备份介质本身也是敏感资产，不能明文存。备份数据加密对备份出来的数据加密后再存放，备份介质即使外泄，没有密钥也无法还原，备份既保险又安全。

一、为什么需要备份数据加密

备份数据往往被分散存放、邮寄或异地保存，比在线数据更容易暴露：

明文备份：备份文件未加密，备份硬盘一旦丢失，数据全部外泄。

流转风险：备份介质邮寄、转运过程中经手环节多，容易丢失。

异地敞放：异地备份点的设备管理不如主机机房严密。

合规压力：含敏感信息的备份明文存放，不满足数据保护要求。

备份加密要让“备份的一份”也锁住：数据加密后再写入备份介质，流转和存放都安全。

二、怎么用

备份任务自动对数据加密。主要环节如下：

表1 备份数据加密流程

环节	系统处理说明
备份加密	执行备份时自动对数据加密
密文落介质	备份介质上保存的是密文
密钥保管	密钥与备份数据分离保管
加密恢复	恢复时凭授权密钥解密还原
全程安全	备份流转与存放均以密文保护

加密对正常备份恢复流程透明：管理员按授权恢复即可。但备份介质一旦遗失，拿到的只是无法读取的密文。执行备份时自动对数据加密，备份介质上保存的是密文，密钥与数据分离保管。恢复时凭授权解密还原，正常流程不受影响，但备份介质流转中即使丢失也不会泄密。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
备份加密	介质丢失不泄露	备份以密文存放，硬盘丢失也读不出内容。
流转安全	邮寄不担心	备份介质转运经手多，加密后即使丢失也安全。
密钥分管	安全可控	密钥与备份数据分离保管，避免单点泄露。
授权恢复	用着不影响	恢复时凭授权解密，正常还原数据。
合规备份	满足要求	加密备份符合敏感数据保护与档案安全规范。
授权恢复	用着不影响	恢复时凭授权解密，正常还原数据。

四、典型使用场景

- 异地备份：备份数据加密后再传往异地，传输存放都安全。
- 介质离机：备份硬盘离机保管，加密防止丢失外泄。
- 敏感档案备份：人事财务等敏感档案的备份加密存储，符合合规。

五、价值与产品定位

备份数据加密给“后备的一份”也上了锁：密文存放、密钥分管、授权恢复，备份介质流转再多也不怕泄密。备份的一份同样上锁，离线介质流转再多也安全，数据保护不留死角。备份介质流转环节多、保管环境也不如主机严密，更需要加密保护。备份出来即密文化，密钥与数据分离，即使介质遗失也不会泄露。离线备份同样安享在线级的安全。加密在备份写出前完成，介质上从无明文留存。密钥与备份数据分离保管，流转再多环节也不失控。离线备份因此获得与在线数据同等的保护力度。

它与档案数据加密、异地容灾、备份恢复协同，使云丰档案在在线存储和离线备份两条线上都实现加密保护，数据安全不留死角。备份介质往往被分散存放、邮寄转运，比在线数据更容易暴露。把备份出来的数据加密后再存，介质即使丢失也读不出内容，密钥与数据分离保管，让离线备份同样安全。备份加密与主存储加密统一密钥管理，不增加额外保管负担。备份介质无论放在机房、异地还是离线柜，都以密文形态存在。流转环节越多，这层保护越显必要。