### 企业办公好用的文档加密软件有哪些？公司视频、数据库、源代码加密有效方案，风奥科技

如今的互联网格局中，数据信息安全对于企业而言发挥的作用越来越大，如何使用好第三方的电子文档加密软件来保护企业内部局域网环境下的数据文件的使用安全？

为什么电子文档加密受到如此的关注度？目前的互联网浪潮中，企业之间的竞争愈来愈大，为了保证企业的数据安全，减少企业数据泄漏的风险，保证企业的核心数据文件的使用安全对于企业而言日益重要。正是因为互联网竞争力的增加，保护好企业的原创版权作品以及相关的知识产权越来越重要。这也是为什么企业加密软件受到互联网企业关注的重要因素和环节。

对于企业来说，除了要加强对内部数据文件的使用安全以外，同时也要加强对局域网内的共享文件，以及外发出去的电子文件和外出办公笔记本电脑上相关数据文件的使用安全，为企业构建全方位的电子文档加密环境，根源杜绝数据泄漏危机。

对于如今的企业来说，主要面临哪些层面的数据泄漏危机？现阶段企业的数据泄漏因素从大的方面主要是分为内部和外部二个方面。对内而言，主要是防止员工有意无意的造成数据泄漏，以及防止内部员工通过聊天工具以及移动存储设备将公司的重要数据文件拷贝带走，造成的一个数据泄漏，其次就是对外的数据泄漏的因素，电脑中毒，企业内部的电脑数据文件被黑客窃取带走，第三方维护人员利用工作便利的条件将相关的数据文件拷贝带走，或者竞争对手窃取商业机密造成企业数据泄漏，将会给企业造成无法挽回的损失。

那么作为企业，如何有效的规避这些数据泄漏的因素，帮助企业构建安全实用的局域网电子文档加密环境？企业如何保证共享数据文件的使用安全？

首先对于企业来说，内部管理人员需要具备一定的安全意识，其次就是关于员工需要具有一定的企业文件使用安全意识。

其次，在基于企业管理人员在具有安全意识的前提下，选择一款适合的第三方电子文档加密软件，在企业的环境下布局好所选择的加密软件，这里以金甲EDS为例，在相关的企业环境调研后的环境下，去为该企业布局金甲企业加密软件的加密环境，然后进行加密软件测试使用，看是否适合企业对于数据文件加密的需求。

接下来，企业提供一台配置合适并且运行速度比较高的电脑，然后在该电脑上安装金甲EDS服务器端，然后进行注册登录，登录后，选择使用说明界面，点击注册，然后联系相关服务商（风奥科技）进行使用注册，注册完成后，可以设置管理员登录的账号密码等等，然后退出，重新登录金甲服务器端，即为完成对金甲服务器的安装。

紧接着，在企业需要安装加密的部门的电脑上进行安装金甲EDS客户端，例如，这里以研发设计部门为例，将所有的研发设计部门的电脑进行加密，那么就需要对研发部门的所有员工使用的电脑安装金甲客户端，然后在金甲服务器上将该部门员工的电脑划分在同一个部门上，方便后期的加密管控以及加密使用。

然后，再次登陆金甲EDS服务器端，进入策略管理界面，然后进行相关的客户端涉密进程勾选，若您公司所需要涉密的进程在策略管理界面没有，那么企业可以自行的添加需要涉密的进程，然后保存更新，进行该策略下的相关加密文件进行安全性的测试使用，看看是否符合企业对于数据安全的需要。

最后，企业在设置好所有的相关策略以后，企业可以根据自身的需求，在金甲EDS服务器上，设置部门加密文件的使用权限、审批解密权限、共享文件的使用权限、外发文件的使用权限、以及U盘使用权限、密文密级策略、明文邮箱的使用权限、离线授权、打印监控等等相关加密权限的设置，这些企业都可以根据自身环境进行使用。

风奥科技，作为国内的重要电子数据文件防泄漏厂商，能够有效的防止电子文件的外泄，根源保证电子数据文件的使用安全，轻松实现对多类型电子文件进行加密管理，有效的防拷贝复制、防文件传传泄露。金甲EDS采用的是Windows底层透明强制性内部文件自动加密保护，经过加密后的相关电子文件在指定环境下可以正常流转使用。未经许可，任何私自拷贝加密文件外发出去，加密后的电子文件都将呈现乱码，或者无法打开。由于企业经常有需要外发的电子文件，风奥金甲企业加密软件为用户提供外发加密管控，以及审批解密操作，有效的管控相关的涉密电子文件在外部环境下的使用安全，控制电子你文件在外部环境下的打开机器、打开次数、打开时间等等操作，例如控制外发文件的使用使用，如果该外发文件的使用时间不在授权范围内，那么加密文件继续呈现加密状态，无法打开。根源防止企业数据文件的使用安全，同时，金甲EDS支持设置对员工电脑文件自动备份，防止恶意删从源头防止企业核心文件被外泄！除造成核心数据的遗失！全方位保证企业电子文件的使用安全，防止数据泄漏事件的发生。