# 安全赋能

**①用户安全等级检查（大于等于 2）/是否独立账号**

账号密码避免弱密码（账号安全等级小于 2 为弱密码），并设置使用人的手机号，密码存储使用密码管理工具，避免写在便签上。
一人一个账号的原则，禁止一个账号多人混用，避免出问题后，难以审计，追责。

**②自定义权限检查-用户组（资料编辑/成本查看/供应商/库存同步/手工下单等）**

**③实施账号是否删除或者授权**

**④是否有人员管理用户及权限功能**

账号权限最小化，只给需要的权限，订单等敏感信息的权限分配需要慎重，避免权限过大导致信息泄漏（临时工账号、导出敏感信息特别要注意）。

**⑤避免不必要的数据导出，导出订单（售后单、出库单）后注意文件的保护，防止文件随意拷贝、随意上传网络**

**⑥员工入职前进行背景调查，离职员工账号及时禁用或删除**

**⑦开启登陆系统的 IP 白名单机制**

有固定 IP 的，请开启登陆系统的 IP 白名单机制，防止账号丢失，异地登陆。

**⑧开通聚水潭开放平台，对获取数据的传输或存储都应进行严格审查，避免数据泄露**

**⑨避免使用来路不明的第三方不正规软件**

办公电脑尽量少安装软件，办公软件从正规渠道获取或者从官方网站下载。

**⑩安装杀毒软件**

推荐杀毒软件：火绒 https://www.huorong.cn/、ESET NOD32 https://www.eset.com.cn/、亚信趋势 https://www.asiainfo-sec.com/。win10 的操作系统也可以用系统自带的杀毒软件。建议只安装一个杀毒软件。

**⑪设置带密码的屏幕保护**

进入“控制面板->显示->屏幕保护程序”，启用屏幕保护程序，设置等待时间为“5 分钟”，并启用“在恢复时显示登陆屏”。

**⑫启用防火墙**

进入“控制面板->网路连接->本地连接”，在高级选项的设置中，启用 windows 自带防火墙，根据业务需要限定允许远程登录该设备的 IP 地址范围。

**⑬及时给操作系统打补丁，保持最新版本**

进入“控制面板->安全和维护->更改安全和维护”，设置成自动更新，并在有更新提示时，不影响工作的情况下及时重启计算机。

**商家 ERP 名称：** **客户签字：**

**时间：** **年** **月** **日**