

## 移动存储设备安全管理解决方案

实现对移动存储介质安全、有效地管理是保证内部敏感信息安全的重要手段。做为信息的载体，移动存储介质具有的灵活、便捷性使它迅速得到普及，越来越多的敏感信息、秘密数据和档案资料被存贮在移动存储介质里，有大量的秘密文件和资料存贮在无保护的移动存储介质中。目前，对于移动存储介质的管理不是非常规范，缺乏严格的保密管理措施，或者是保密管理措施不具体，有的甚至根本未被纳入保密管理范畴：如对涉密软盘、磁盘、移动硬盘等没有登记，没有加密标识，与普通磁盘混合使用，出现故障后随便丢弃或重新格式化后继续使用等。这些现象无疑给单位内部的涉密和敏感信息资源带来了相当大的安全隐患。

### ● 安全风险分析：

- 1) 工作人员在单位内部使用未纳入管理的个人 U 盘、移动硬盘、软盘或光盘等，容易携带各种计算机病毒或恶意代码，造成病毒传播和泛滥；
- 2) 怀有恶意的内部工作人员很容易使用 U 盘等移动存储介质将单位的重要数据拷贝带出，造成单位敏感信息或商业秘密外泄；
- 3) 移动存储介质一旦丢失或者被盗，存储在介质上的内部敏感数据或文件很容易失控，造成信息泄密；

### ● 解决方案：

中安源移动存储设备安全管理系统主要通过移动存储介质注册授权、权限管理、访问控制、数据保护等多种手段，防止外部非法移动介质在内网中使用，防止内部移动存储介质因丢失等原因造成的信息泄密，并通过对内网移动存储介质的统一管理，记录移动存储介质的使用情况，做到内部移动存储介质的可控可管。主要功能如下：

- 1) 支持各种类型的移动存储介质，包括 U 盘、移动硬盘、软盘、MO 和外挂 IDE 硬盘等；
- 2) 提供对移动存储介质的注册管理功能，没有经过管理员注册的移动存

储介质，不能在单位内部计算机上使用。移动存储介质要获得使用权，必须经过管理员注册，并赋予相应的权限。管理员还可以取消对移动存储介质的注册，收回对该移动存储介质的特殊授权。

- 3) 根据管理需要，管理员可以将特定的移动存储介质注册授权给特定的用户/用户组和特定的计算机/计算机组，从而实现灵活的细粒度管理。
- 4) 对移动存储介质的权限可分为禁用、只读、安全读写和正常读写四种。
- 5) 对于高安全级别的移动存储介质，可将其使用范围严格锁定在内部工作环境中，在外部网络计算机上无法使用注册过的内部移动存储介质，实现内外网移动存储介质的双向隔离；
- 6) 对于机密级别较高的移动存储介质，系统还提供了数据保护功能，即所有写入移动存储介质的数据都会被自动加密；用户在读取文件时，数据能够被自动解密。
- 7) 提供详细的审计记录，包括注册信息、使用信息和文件操作信息，记录要素包括使用人、使用计算机、使用时间和动作等，并提供丰富的审计报告。

● 系统部署示意图：

