**XXX单位**

**介质管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479446302)

[2 适用范围 1](#_Toc479446303)

[3 介质管理 1](#_Toc479446304)

[4 安全管理 1](#_Toc479446305)

[4.1 购置、收发 2](#_Toc479446306)

[4.2 使用 2](#_Toc479446307)

[4.3 报废与处理 2](#_Toc479446308)

[5 附则 3](#_Toc479446309)

# 目的

为规范XXX单位信息系统的介质安全管理，特制定本制度。

# 适用范围

本制度适用于XXX单位信息系统介质管理。

# 介质管理

应建立介质安全管理制度，对介质标识、介质传递、介质访问、介质保管和介质销毁等方面进行管理规定。

应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理。

应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。

应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

应部署统一介质管理软件，实现客户端移动介质的统一管理。

移动介质在使用前，必须进行杀毒处理，防止病毒入侵。

禁止将内部移动介质带出使用，防止数据泄露。

应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁。

# 安全管理

移动介质是指通过专用注册工具对普通的移动存储介质（主要为移动硬盘、U盘）内数据经过高强度算法加密，并根据安全控制策略的需要进行数据区划分，使其具有较高安全性能的移动存储介质。

移动介质的管理，遵循“统一购置、统一标识、统一备案、跟踪管理”的原则，严格控制发放范围。

## 购置、收发

信息化管理部门购置、收发存储介质时，要严格履行清点、登记、编号、签收等手续。涉密介质应在显眼的位置做出“绝密”、“机密”、“秘密”的密级标识。介质密级的确定依据其存储信息的最高密级。

各单位需要使用移动介质的内部人员，应进行领用登记。传递涉密存储介质时，应当包装密封，并且标明密级、编号和收发件单位名称。

## 使用

移动介质的管理原则是：“谁使用，谁负责”。介质使用人员对所使用的存储介质负责。

用户将移动电子介质接入税务网络和信息系统前，必须进行病毒、木马检测和杀毒处理，防止病毒侵入侵和传染。

外来存储介质未经本单位信息化管理部门授权不得擅自接入、拷贝、记录、打印云南地税系统内部信息。确需使用时，应向本单位信息化管理部门登记。

存储有内部重要或敏感信息的移动介质应安排专人进行妥善保管，未经授权不得将载有敏感信息的存储介质随意存放或带出办公地点。

用户不得在内网与外网之间交叉使用存储介质。

在移动介质使用过程中，应当注意检查病毒、木马等恶意代码，注意远离水源、火源，避免接触强磁物体、避免阳光直接照射。

## 报废与处理

移动质记录的信息如果不再需要或介质弃用时，须立即清除信息。

移动介质涉密信息的清除，除考虑删除、格式化等方式外，还要进行数据覆盖写入等操作；

移动介质弃用时，还要考虑借助专业软件多次格式化、物理破坏、物理粉碎、消磁等操作。

如安全移动存储介质不慎遗失，当事人应立即报本科室负责人，及时采取有效措施，防止信息泄密，如有泄密由当事人负全部责任，同时应报信息技术科进行登记备案。

各工作人员离岗、离职前，应将统一配发的安全移动存储介质退还信息技术科并办理相关手续。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。