

信息资产管理办法（试行）

第一章 总 则

第一条 本管理制度的主要目的是对信息资产进行安全管理，落实资产的安全责任，明确资产管理流程，具体为：

（一）通过对信息资产进行合理的等级分类，为信息资产管理提供科学、有效的方式；

（二）对现有信息资产进行信息安全属性的赋值，并对其进行等级划分，从而进行有针对性地保护，同时为以后的安全解决方案提供依据。

第二条 本管理制度适用于贵州交通技师学院所管理的所有信息资产和全体信息工作人员。

第二章 信息资产责任

第三条 网络综合治理、网络安全和信息化领导小组办公室（以下简称网信小组）是贵州交通技师学院信息资产安全管理工作的最高领导机构，负责统筹规划、协调与监督全院信息资产的管理工作，各部门及系（部）负责人指定本部门信息资产的责任人，负责组织落实本部门信息资产的日常工作，确保资产的合理使用、安全保管与及时登记上报。

第四条 信息资产应明确其所有者、管理者及使用者三类角色。

第五条 信息资产所有者是指对资产具有所有权的单位、部门或个人，信息资产所有者对资产的获取、使用及处

置具有最高决策权；信息资产的管理者通常可以是信息资产的所有者，也可以是得到信息资产所有者授权的其他部门或个人，信息资产管理者根据信息资产所有者的授权行使对信息资产的日常管理，对于超出授权范围的管理要求，需要单独向所有者申请相应权限。

第六条 对于具有多个所有者或管理者的信息资产，由网信小组根据实际工作需要，指定一个唯一的所有者或管理者。

第三章 信息资产分类

第七条 贵州交通技师学院的信息资产包括以下五类：

（一）文档与数据类资产：数据库和数据文件、合同和协议、系统文件、程序代码、用户手册、培训材料、操作或支持程序、业务连续性计划、审计记录、归档的信息；

（二）硬件与设备类资产：包括计算机终端（台式机、笔记本电脑）、服务器、存储设备、网络设备（路由器、交换机、防火墙等）、机房专用设备（UPS、精密空调等）、输入输出设备（打印机、扫描仪、投影仪等）以及各类移动终端设备等；

（三）软件与系统类资产：涵盖操作系统软件（Windows、Linux 等）、办公软件（Office 套件、WPS 等）、专业应用软件（如 CAD、汽修诊断软件等学院教学科研所需软件）、数据库软件（Oracle、MySQL 等）、中间件软件以及各类工

具软件；分为自主研发软件、外购商用软件与开源软件，按不同来源分别管理；

（四）网络资源：包括学院内外部网络接入线路（如光纤专线、宽带链路）、IP 地址资源、域名资源、无线网络覆盖设施及网络服务（如电子邮件、校内网站空间等），统一规划、分配与管理网络资源，保障网络互联互通与安全访问。

第四章 信息资产分级和标识管理

第八条 根据《贵州交通技师学院(贵州省交通运输学校)数据安全管理办法》对信息资产的分级为 5 级：核心、重要、敏感、内部、公开。

（一）核心：是最重要的贵州交通技师学院资产，一旦损坏或泄露会使贵州交通技师学院的安全、权益和利益遭受特别严重的损害。

（二）重要：是重要的贵州交通技师学院资产，一旦损坏或泄露会使贵州交通技师学院的安全、权益和利益遭受严重的损害，给贵州交通技师学院造成重大损失。

（三）敏感：是不宜公开对外的，公开后会对贵州交通技师学院的安全、形象、权益和利益产生不利后果的敏感文件、信息和材料。

（四）内部：是不宜公开对外的，非授权的公开、泄露将直接对学院、学生或者员工造成较小影响的文件、信息和材料。

（五）公开：包含可对社会公开的信息，公用的信息处理设备和系统资源等。

第九条 对信息资产的标识方法如下：

（一）对“内部”和“公开”信息资产须进行标识，对“敏感”“重要”和“核心”信息资产须进行标识和声明。

（二）对于文件形式的信息资产，须由信息资产管理者在文件明显位置标识其类别、级别、失效日期（失效日期指信息级别的有效性截止日期。到达失效日期后，应对信息进行重新定级，否则默认为“公开”信息）等，且文件和标识不能分开。标识应该醒目，标识格式应统一，标识方法应便于检查。对于非文件形式的“敏感”“重要”和“核心”信息，如无法标识，必须声明。

（三）对于“敏感”“重要”和“核心”信息，须由管理者对信息资产名称、类别、级别、失效日期等以声明文件的形式进行声明，声明文件须由网信小组审核签字。声明文件须跟随信息资产一起保管和传递。

（四）多个不同级别的信息资产合并在一起时，按最高级别给混合信息资产进行标识和声明。

第五章 信息资产使用管理

第十条 严格禁止内部工作人员和外部人员对“核心”类资产的非授权访问，一旦发现有对“核心”类信息的非授权使用，必须立即作为安全事件向信息安全管理组报告，核实后上报网信小组。

第十一条 对“核心”类资产的授权使用过程中须注意以下事项：

（一）核心文件必须放在有安全保障的防火保险柜内加锁保存，并由专人保管；传阅核心文件时，必须严格限制在文件规定的发放范围内，使用者在内部阅读时需要签名登记，阅读完毕要及时收回；

（二）对于核心类应用系统需要采取严格的授权和强审计的留痕机制。

（三）对于含有核心信息的系统，建议在适当的地点建立物理隔离和网络逻辑隔离的使用环境；

（四）禁止在网络上传送核心类电子数据；

（五）对核心类数据的存储要建立强逻辑访问控制机制；要进行可靠的备份，并定期进行测试；要采用严格的物理访问控制，信息应当被存储在采取物理保护措施的计算机上；

（六）含核心信息的纸质文件不得重复使用，纸质文件要通过专用设备彻底粉碎或烧毁；电子文件要使用专门的清除软件安全清除；存储介质需要可靠地擦除或物理上彻底销毁；

（七）我校将对有意或无意地暴露核心信息的行为进行处罚，对于性质严重，危害较大的事件，触及法律的，由司法机关处理。

第十二条 “重要”类资产是一类极其敏感的资产。对贵州交通技师学院来说，在没有相应授权的前提下，严格禁止内部工作人员和外部人员对“重要”类资产的访问，一旦

发现有对“重要”类信息的非授权使用，必须立即作为安全事件向本部门信息安全责任人或本部门主管领导报告，核实后上报信息安全管理组。

第十三条 对“重要”类资产的授权使用过程中须注意以下事项：

（一）重要文件必须放在有安全保障的库房或文件柜内加锁保存，并由专人保管；传阅重要文件时，必须严格限制在文件规定的范围内，使用者在内部阅读时需要签名登记，阅读完毕要及时收回；

（二）对于重要类应用系统需要采取严格的授权和强审计的留痕机制；

（三）对于含有重要性信息的系统，建议在适当的地点建立物理隔离的使用环境；

（四）禁止在网络上传送未加密的重要类电子数据；

（五）对重要类数据的存储要建立强逻辑访问控制机制；要进行可靠的备份，并定期进行测试；要采用严格的物理访问控制，信息应当被存储在采取物理保护措施的计算机上；

（六）含重要信息的纸件不得重复使用，纸质文件要通过专用设备彻底粉碎或烧毁；电子文件要使用专门的清除软件安全清除；存储介质需要可靠地擦除或物理上彻底销毁；

（七）我校将对有意或无意地暴露重要信息的行为进行处罚，对于性质严重，危害较大的事件，触及法律的，由司法机关处理。

第十四条 “敏感”类资产仅限于贵州交通技师学院内部工作人员使用，一般避免向外扩散，外部人员要使用“敏感”类信息，需要得到必要的授权。

第十五条 对“敏感”类资产的授权使用过程中须注意以下事项：

（一）内部工作人员使用与其工作相关的“敏感”类数据没有限制；

（二）对于敏感类应用系统需要根据访问控制要求为使用用户分配用户名和口令；

（三）“敏感”类信息可以在贵州交通技师学院的所有内部网络上使用，但禁止在外网上传送；

（四）对敏感类数据的存储要建立逻辑访问控制机制；要进行可靠的备份，并定期进行测试；

（六）含敏感信息的纸质文件要通过专用设备彻底粉碎或烧毁；电子文件要使用专门的清除软件安全清除；存储介质需要可靠地擦除或物理上彻底销毁；

（七）我校将对有意或无意地暴露一般信息的行为进行处罚。

第十六条 “内部”类资产是指类资产仅限于贵州交通技师学院内部工作人员使用，外部人员要使用“敏感”类信息，需要得到必要的授权。

第十七条 对“内部”类资产的授权使用过程中须注意以下事项：

（一）内部工作人员使用“内部”类数据没有限制；

（二）对于内部类应用系统需要根据访问控制要求为使用用户分配用户名和口令；

（三）对内部类数据的存储要建立逻辑访问控制机制；要进行可靠的备份，并定期进行测试；

（六）含内部信息的纸质文件要通过专用设备彻底粉碎或烧毁；电子文件要使用专门的清除软件安全清除；存储介质需要可靠地擦除或物理上彻底销毁；

（七）我校将对有意或无意地暴露内部信息的行为进行处罚。

第十八条 “公开”类资产是指可以公共访问的资产和对外发布的信息，并且信息可以自由散布而不会产生任何安全问题。

第十九条 “公开”类文件可以向第三方人员公开，并允许对外进行发布，但是必须注明一般信息的来源出处；应将资产的访问权限设为“只读”，只对少数需要修改、更新公开信息的人员开放“写”和“删除”的权限。

第六章 信息资产清单管理

第二十条 信息资产清单必须详细记录贵州交通技师学院所有的各类信息资产，其内容包括信息资产分类、信息资产编号、资产名称、资产描述、资产位置、资产所有者、管理者、使用者、重要程度等内容。

第二十一条 信息资产管理员负责维护和保存贵州交通技师学院的信息资产清单，并定期检查信息资产清单的正确

性和完整性；在信息资产发生变更时在教育系统网络安全工作管理平台及时动态更新资产清单。

第七章 附 则

第二十二条 本管理制度的解释和修改权属于网信小组。

第二十三条 本管理制度自发布之日起执行。