

客户信息保密管理规定

客户信息保密管理规定（通用 9 篇）

现如今，很多场合都离不开制度，制度是一种要求大家共同遵守的规章或准则。你所接触过的制度都是什么样子的呢？以下是店铺整理的客户信息保密管理规定，希望对大家有所帮助。

客户信息保密管理规定 篇 1

1、目的

为保证公司客户信息安全，防止客户信息失密泄密事件发生，特制定本制度。

2、范围

适用于公司内全体员工。

3、职责

3.1 品质管理部负责制度的拟定和对执行情况的监督；

3.2 各部门负责人负责客户信息清单编制、保管，对客户信息人员监督工作。

3.3 各部门负责对本部门客户信息的日常管理。

3.4 各服务中心项目经理

3.4.1 负责纸质客户信息打印申请批示。

3.4.2 监督部门人员实行客户信息保密工作。

3.5 总经理负责客户信息需提供于公司外部使用时批示。

4、术语定义

客户信息属于公司秘密信息，公司秘密是指关系公司的利益，依照一定程序确定，在一定时间内只限一定范围的人员知悉的，经公司采取保密措施并具有实用性的信息。

5、方法和过程控制

5.1 客户信息分类

5.1.1 纸质信息

交付时产生的客户档案或其他信息。

5.1.2 电子信息

各种格式电子客户信息。

5.1.3 管控数据

指管控系统中客户资料。

5.2 客户信息权限、使用、保管、销毁

5.2.1 纸质信息

5.2.1.1 除客户档案外不得保留任何形式的纸质客户信息。特殊情况需经部门经理负责人批示后方可打印，打印件盖“受控文件”、使用期限后接收人签收领取。

5.2.1.2 使用过程中不得转借他人，不得带出办公区域。

5.2.2 电子信息

5.2.2.1 交付时由地产提供电子版客户资料只能由项目负责人保管，若信息员因工作需要，项目负责人可授权给信息员使用。但需设置权限只能查看，不能打印、复制、转发。

5.2.2.2 当信息员结合客户档案、地产提供的电子版客户资料完成管控数据的建立并确认无误后，信息员与项目负责人保留的电子信息均需销毁处理。

5.2.2.3 销毁需由项目负责人监销并记录。

5.2.2.4 包括但不限于大范围访谈、人口普查所产生的纸质客户信息，由信息员与管控进行核对，及时更新，核对完后，再由客户经理将客户的其他诉求信息进行电子版归档管理，但不得保留客户电话、工作单位等私密信息。

5.2.3 管控数据

5.2.3.1 品质管理部 IT 工程师有管控全部权限。

5.2.3.2 各项目信息员有除客户信息导入导出外的所有权限。

5.2.3.3 其他有管控使用需要人员只有录入、查看权限。

5.2.4 各部门根据实际使用情况评估客户信息外泄风险，决定是否封闭相关计算机 **USB** 接口、刻录光驱。

5.2.5 新员工入职需鉴定保密协议，离职时做好相关移交、注销工作。

5.3 监督检查

5.3.1 各部门需每月对客户信息保密风险进行一次评估，并及时整改。

5.3.2 品质管理部每两个月对各项目客户信息保密工作进行一次检查。对存在重大隐患的项目进行通报批评。

5.3.3 凡有下列表现之一的公司员工，公司根据其贡献给予奖励100-1000 元；

(1)对泄露或者非法获取公司客户信息的行为，及时检举的；

(2)发现他人泄露或者可能泄露公司客户信息，立即采取补救措施，避免或者减轻了损失后果的；

5.3.4 凡有下列情形之一，给予罚款 300-2000 元，如情节严重，给予辞职，赔偿公司经济损失：

(1)因疏忽大意而泄露公司客户信息。

(2)遗失书面客户信息清单。

(3)出卖公司利益，利用公司客户信息为自己谋利的，除赔偿公司经济损失外，还要交司法部门处理。

6、 相关文件

无

7、 相关记录菜单

《客户信息保密风险评估表》

《客户信息借阅、销毁记录表》

客户信息保密管理规定 篇2

一、总则

为使公司对客户的管理规范化、有效化，保证稳定开展，特制定本办法。

二、客户界定

公司客户为与公司有业务往来的供应商和经销商。

公司有关的律师、、广告、公关、银行、保险、融资协助机构，可列为特殊的一类客户。

三、客户信息管理

公司营销部（、信息部）负责公司所有客户信息、资料、数据的

分类、汇总、整理。

公司建立客户档案，指定专人负责，规定统一格式、内容，并编制客户一览表供查阅。

四、客户档案的建立

1. 每发展、接触一个新客户，均应建立客户档案户头。

2. 客户档案适当标准化、规范化，摸清客户基本信息，如客户名称、法定代表人或法人代表、地址、邮编、电话、传真、经营范围、注册资本等。

3. 客户档案资料、信息、数据要做到定期更新、修改。

4. 客户单位的发生重大变动事项、与本公司的业务交往，均须记入客户档案。

5. 积累客户年度业绩和财务状况报告。

五、公司各部门与客户接触的，均须报告所辖部门（除该业务保密外），不得局限在业务人员个人范围内。

六、员工调离公司时，不得将客户资料带走，其主管部门将其客户资料接收、整理、归档。

七、建立客户信息查阅权限制，未经许可，不得随意调阅客户档案。

八、客户管理

接待客户，按公司对外接待办法处理，对重要的客户按贵宾级别接待。

与客户的信函、传真、长话交往，均应按公司各项管理办法记录在案，并整合在客户档案内。

对一些较重要、未来将发展的新客户，公司要有两个以上的人员与之联系，并建立联系报告制。

负责与客户联系的员工调离公司时，应由公司及时通知有关客户，并指派其员工顶替调离员工迅速与客户建立联系。

九.附则

本办法由营销部（、信息部）解释、补充，经总经理批准颁行。

例：客户信息错误后怎么管理

先由客服部人员制订补救处理方案，交由客服部经理审核，客服经理审核后再交由总经理审批，总经理审批后转回客服部组织执行，客服部再交接给其他部门执行，其他部门执行后反馈意见给客服部，客服部再写报告交由客服经理审核，客服经理再交给总经理审批，总经理审批后存档，结束。

客户信息保密管理规定 篇3

一、总则

为加强公司保密工作的管理，防范和杜绝各种泄密事件的发生，维护公司正常经营管理秩序，保障公司合法权益不受侵犯，特制定本制度。

二、适用范围

本制度适用于总公司及直属公司全体员工，每个员工均有保守公司秘密的义务和制止他人泄密的权利。

三、保密范围和密级划分

公司秘密指涉及公司利益、依照一定程序确定、在一定时间内只限一定范围内的人员知悉的事项。

1、密级划分

公司秘密的密级分为绝密、机密、秘密三级。

1)绝密级:是最重要的公司秘密，泄露会给公司造成特别严重的经济损失或不良影响；

2)机密级:是重要的公司秘密，泄露会给公司造成严重的经济损失或不良影响；

3)秘密级:是一般的公司秘密，泄露会给公司造成经济损失或不良影响。

2、保密范围

公司秘密包括下列事项：

1)公司重大决策中的秘密事项；

2)公司尚未付诸实施的经营战略、经营方向、经营规划、经营项目及经营决策；

3)公司的合同、协议、意见书及可行性报告、重要会议记录；

- 4)公司财务预决算报告、审计报告及各类财务报表、统计报表;
- 5)公司所掌握的尚未进入市场或尚未公开的各类信息;
- 6)公司的管理策略、客户信息、货源情报、产销策略;
- 7)公司技术水平、技术力量、技术潜力、产品动向;
- 8)公司持有、掌握的厂家技术资料、光盘、书籍、文档;
- 9)公司营业执照、组织机构代码证、税务登记证等相关证件;
- 10)公司员工的人事档案、工资、奖金及相关资料;
- 11)其他经公司确认应当保密的事项。

一般性决定、决议、通告、通知、行政管理资料等内部文件不属于保密范围。

3、公司密级的确定

- 1)公司经营发展中,直接影响公司权益和利益的重要决策文件、资料为绝密级;
- 2)公司的年度规划、财务报表、统计资料、重要会议记录、公司经营情况、厂家技术资料为机密级;
- 3)公司合同、协议、人事档案、工资、奖金、尚未进入市场或尚未公开的各类信息、营业执照及相关证件为秘密级。

4、属于公司秘密的文件、资料,由起草公司或部门依据本制度第三项“保密范围和密级划分”中的第1条密级划分、第3条公司密级的确定的规定标明密级,并确定保密期限。保密期限届满,除要求继续保密的事项外,自行解密。

四、保密管理

1、知晓范围

- 1)公司秘密(绝密、机密、秘密)总公司副/总经理有权全部知晓;2)绝密级只限总公司副/总经理指定的人员知晓;
- 3)机密级只限负责该项工作的主管人员以及该主管人员认为必须知道的人员知晓;
- 4)秘密级只限相关人员知晓。

2、保管备份

- 1)绝密级资料原则上不允许摘抄或复制,确需摘抄或复制者须经

总公司副/总经理批准；

2)机密级、秘密级资料需经子公司总经理批准后，方可摘抄或复制；3)保密资料不得私自复制，复印件应视同原件管理；

4)各公司保管的公司证件需经子公司总经理批准后，方可复印或借出(营业执照、组织机构代码证经部门经理批准后，可复印)；

5)各公司指派专人负责秘密文件、资料的保管，并采用相应的保密措施；6)若发现或发生泄密情况，应立即向总公司领导报告，以便及时采取补救措施。

五、责任与奖惩

1、有下列情形之一者，对有关部门或人员给予奖励：

1)及时举报泄密事件，且避免可能由此造成公司损失的；

2)非责任人及时采取补救措施，避免或最大限度减少泄密造成损失的。

2、有下列情形之一者，对有关部门或人员给予处罚，情节严重的，将依法追究相关法律责任：

1)泄露公司秘密，尚未造成严重后果或经济损失的；

2)故意或过失泄露公司秘密，造成严重后果或重大经济损失的；

3)违反本制度规定，为他人窃取、刺探、收买或提供公司秘密的；

4)利用职权强制他人违反保密规定的。

3、奖惩具体标准参照员工奖惩管理制度执行。

六、本制度自发布之日起生效。

七、本制度的解释归人力资源部所有。

客户信息保密管理规定 篇4

第一章 总则

第一条 为加强邮政行业寄递服务用户个人信息安全管理，保护用户合法权益，维护邮政通信与信息的安全，促进邮政行业健康发展，根据《中华人民共和国邮政法》、《全国人大常委会关于加强网络信息保护的规定》、《邮政行业安全监督管理办法》等法律、行政法规和有关规定，制定本规定。

第二条 在中华人民共和国境内经营和使用寄递服务涉及用户个人

信息安全的活动以及相关监督管理工作，适用本规定。

第三条 本规定所称寄递服务用户个人信息（以下简称寄递用户信息），是指用户在使用寄递服务过程中的个人信息，包括寄（收）件人的姓名、地址、身份证件号码、电话号码、单位名称，以及寄递详情单号、时间、物品明细等内容。

第四条 寄递用户信息安全监督管理坚持安全第一、预防为主、综合治理的方针，保障用户个人信息安全。

第五条 国务院邮政管理部门负责全国邮政行业寄递用户信息安全监督管理工作。

省、自治区、直辖市邮政管理机构负责本行政区域内的邮政行业寄递用户信息安全监督管理工作。

按照国务院规定设立的省级以下邮政管理机构负责本辖区的邮政行业寄递用户信息安全监督管理工作。

国务院邮政管理部门和省、自治区、直辖市邮政管理机构以及省级以下邮政管理机构，统称为邮政管理部门。

第六条 邮政管理部门应当与有关部门相互配合，健全寄递用户信息安全保障机制，维护寄递用户信息安全。

第七条 邮政企业、快递企业及其从业人员应当遵守国家有关信息安全管理的规定及本规定，防止寄递用户信息泄露、丢失。

第二章 一般规定

第八条 邮政企业、快递企业应当建立健全寄递用户信息安全保障制度和措施，明确企业内部各部门、岗位的安全责任，加强寄递用户信息安全管理 and 安全责任考核。

第九条 以加盟方式经营快递业务企业应当在加盟协议中订立寄递用户信息安全保障条款，明确被加盟人与加盟人的安全责任。加盟人发生信息安全事故时，被加盟人应当依法承担相应安全管理责任。

第十条 邮政企业、快递企业应当与其从业人员签订寄递用户信息保密协议，明确保密义务和违约责任。

第十一条 邮政企业、快递企业应当组织从业人员进行寄递用户信息安全保护相关知识、技能培训，加强职业道德教育，不断提高从业

人员的法制观念和责任意识。

第十二条 邮政企业、快递企业应当建立寄递用户信息安全投诉处理机制，公布有效联系方式，接受并及时处理有关投诉。

第十三条 邮政企业、快递企业受网络购物、电视购物和邮购等经营者委托提供寄递服务的，在与委托方签订协议时，应当订立寄递用户信息安全保障条款，明确信息使用范围和方式、信息交换安全保护措施、信息泄露责任划分等内容。

第十四条 邮政企业、快递企业委托第三方录入寄递用户信息的，应当确认其具有信息安全保障能力，并订立信息安全保障条款，明确责任划分。第三方发生信息安全事故导致寄递用户信息泄露、丢失的，邮政企业、快递企业应当依法承担相应责任。

第十五条 未经法律明确授权或者用户书面同意，邮政企业、快递企业及其从业人员不得将其掌握的寄递用户信息提供给任何单位或者个人。

第十六条 公安机关、国家安全机关或者检察机关的工作人员依照法律规定程序调阅、检查寄递详情单实物及电子信息档案，邮政企业、快递企业应当配合，并对有关情况予以保密。

第十七条 邮政企业、快递企业应当建立寄递用户信息安全应急处置机制。对于突发的寄递用户信息安全事故，应当立即采取补救措施，按照规定报告邮政管理部门，并配合邮政管理部门和相关部门的调查处理工作，不得迟报、漏报、谎报、瞒报。

第三章 寄递详情单实物信息安全管理

第十八条 邮政企业、快递企业应当加强寄递详情单管理，对空白寄递详情单发放情况进行登记，对号段进行全程跟踪，形成跟踪记录。

第十九条 邮政企业、快递企业应当加强营业场所、处理场所管理，严禁无关人员进出邮件（快件）处理、存放场地，严禁无关人员接触、翻阅邮件（快件），防止寄递详情单实物信息（以下简称实物信息）在处理过程中泄露。

第二十条 邮政企业、快递企业应当优化寄递处理流程，减少接触实物信息的处理环节和操作人员。

邮政企业、快递企业应当采用有效技术手段，防止实物信息在寄递过程中泄露。

第二十二条 邮政企业、快递企业应当配备符合国家标准的安全监控设备，安排具有专门技术和技能的人员，对收寄、分拣、运输、投递等环节的实物信息处理进行安全监控。

第二十三条 邮政企业、快递企业应当建立健全寄递详情单实物档案管理制度，实行集中封闭管理，确定集中存放地，及时回收寄递详情单妥善保管。设立、变更集中存放地，应当及时报告所在地邮政管理部门。

第二十四条 邮政企业、快递企业应当对寄递详情单实物档案集中存放地设专人管理，采取必要的安全防护措施，确保存储安全。

第二十五条 邮政企业、快递企业应当建立并严格执行寄递详情单实物档案查询管理制度。内部人员因工作需要查阅档案时，应当确保档案完整无损，并做好查阅登记，不得私自携带离开存放地。

第二十六条 寄递详情单实物档案应当按照国家相关标准规定的期限保存。保存期满后，由企业集中销毁，做好销毁记录，严禁丢弃或者贩卖。

第二十七条 邮政企业、快递企业应当对实物信息安全保障情况进行定期自查，记录自查情况，及时消除自查中发现的信息安全隐患。

第四章 寄递详情单电子信息安全管理

第二十八条 邮政企业、快递企业应当按照国家规定，加强寄递服务用户信息相关信息系统和网络设施的安全管理。

第二十九条 邮政企业、快递企业信息系统的网络架构应当符合国家信息安全管理规定，合理划分安全区域，实现各安全区域之间有效隔离，并具有防范、监控和阻断来自内部和外部网络攻击破坏的能力。

第三十条 邮政企业、快递企业应当配备必要的防病毒软件、硬件，确保信息系统和网络具有防范计算机病毒的能力，防止恶意代码破坏信息系统和网络，避免信息泄露或者被篡改。

第三十一条 邮政企业、快递企业构建信息系统和网络，应当避免使用信息系统和网络供应商提供的默认密码、安全参数，并对通过开

息系统、网络设备的远程访问。

第三十二条 邮政企业、快递企业在采购计算机软件、硬件产品或者技术服务时，应当与供应商签订保密协议，明确其安全责任，以及在发生信息安全事件时配合邮政管理部门和相关部门调查的义务。

第三十三条 邮政企业、快递企业应当建立信息系统安全内部审计制度，定期开展内部审计，对发现的问题及时整改。

第三十四条 邮政企业、快递企业应当加强信息系统及网络的权限管理，基于权限最小化和权限分离原则，向从业人员分配满足工作需要s的最小操作权限和可访问的最小信息范围。

邮政企业、快递企业应当加强对信息系统和数据库的管理，使网络管理人员仅具有进行信息系统、数据库、网络运行维护和优化的权限。网络管理人员的维护操作须经安全管理员授权，并受到安全审计员的监控和审计。

第三十五条 邮政企业、快递企业应当加强信息系统密码管理，使用高安全级别密码策略，定期更换密码，禁止将密码透露给无关人员。

第三十六条 邮政企业、快递企业应当加强寄递用户电子信息的存储安全管理，包括：

（一）使用独立物理区域存储寄递用户信息，禁止非授权人员进出该区域；

（二）采用加密方式存储寄递用户信息；

（三）确保安全使用、保管和处置存有寄递用户信息的计算机、移动设备和移动存储介质。明确管理数据存储设备、介质的负责人，建立设备、介质使用和借用登记制度，限制设备输出接口的使用。存储设备和介质报废的，应当及时删除其中的寄递用户信息数据，并销毁硬件。

第三十七条 邮政企业、快递企业应当加强寄递用户信息的应用安全管理，对所有批量导出、复制、销毁用户个人信息的操作进行审查，并采取防泄密措施，同时记录进行操作的人员、时间、地点和事项，留作信息安全审计依据。

邮政企业、快递企业应当加强对离岗人员的信息安全审计，及时删除或者禁用离岗人员系统账户。

第三十九条 邮政企业、快递企业应当制定本企业与市场相关主体的信息系统安全互联技术规则，对存储寄递服务信息的信息系统实行接入审查，定期进行安全风险评估。

第五章 监督管理

第四十条 邮政管理部门依法履行下列职责：

（一）制定保障寄递用户信息安全的政策、制度和相关标准，并监督实施；

（二）监督、指导邮政企业、快递企业落实信息安全责任制，督促企业加强寄递用户信息安全管理；

（三）对寄递用户信息安全进行监测、预警和应急管理；

（四）监督、指导邮政企业、快递企业开展寄递用户信息安全宣传教育和培训；

（五）依法对邮政企业、快递企业实施寄递用户信息安全监督检查；

（六）组织调查或者参与调查寄递用户信息安全事故，依法查处违反寄递用户信息安全管理规定的行为；

（七）法律、行政法规和规章规定的其他职责。

第四十一条 邮政管理部门应当加强邮政行业寄递用户信息安全管理制度和知识的宣传，强化邮政企业、快递企业及其从业人员的信息安全管理意识，提高用户对个人信息安全保护的认识。

第四十二条 邮政管理部门应当加强邮政行业寄递用户信息安全运行的监测预警，建立信息管理体系，收集、分析与信息安全有关的各类信息。

下级邮政管理部门应当及时向上一级邮政管理部门报告邮政行业寄递用户信息安全情况，并根据需要通报工业和信息化、通信管理、公安、国家安全、商务和工商行政管理等相关部门。

第四十三条 邮政管理部门应当对邮政企业、快递企业建立和执行寄递用户信息安全管理制度，规范从业人员信息安全保护行为，防范

第四十四条 邮政管理部门发现邮政企业、快递企业存在违反寄递用户信息安全管理规定，妨害或者可能妨害寄递用户信息安全的，应当依法进行调查处理。违法行为涉及其他部门管理职权的，邮政管理部门应当会同有关部门对涉案邮政企业、快递企业进行调查处理。

第四十五条 邮政管理部门应当加强对邮政企业、快递企业及其从业人员遵守本规定情况的监督检查。

第四十六条 邮政企业、快递企业拒不配合寄递用户信息安全监督检查的，依照《中华人民共和国邮政法》第七十七条的规定予以处罚。

第四十七条 邮政企业、快递企业及其从业人员因泄露寄递用户信息对用户造成损失的，应当依法予以赔偿。

第四十八条 邮政企业、快递企业及其从业人员违法提供寄递用户信息，尚未构成犯罪的，依照《中华人民共和国邮政法》第七十六条的规定予以处罚。构成犯罪的，移送司法机关追究刑事责任。

第四十九条 任何单位和个人有权向邮政管理部门举报违反本规定的行为。邮政管理部门接到举报后，应当依法及时处理。

第五十条 邮政管理部门可以在行业内通报邮政企业、快递企业违反寄递用户信息安全管理规定行为、信息安全事件，以及对有关责任人员进行处理的情况。必要时可以向社会公布上述信息，但涉及国家秘密、商业秘密和个人隐私的除外。

第五十一条 邮政管理部门及其工作人员对在履行职责过程中知悉的寄递用户信息应当保密，不得泄露、篡改或者损毁，不得出售或者非法向他人提供。

第五十二条 邮政管理部门工作人员在寄递用户信息安全管理工作中滥用、玩忽职守，依照《邮政行业安全监督管理办法》第五十五条的规定予以处理。

第六章 附 则

第五十三条 本规定自发布之日起施行。

篇 5

第一章

证文书档案、声像档案的及时归档和妥善保管，特制度本规定。

第二条行政助理负责档案的归档监督和日常管理工作。对档案资料必须按年度立卷，各系统和部门在工作活动中形成的各种有保存价值的档案资料，都要按本制度规定分别立卷归档。

第三条坚持部门收集保管、定期、及时归档制度。各系统和部门负责人均应制定专人负责收集保管本系统或本部门的档案资料并监督其及时归档。名单报总经理办公室档案室备案，如需变动应及时通知档案管理人员。因工作变动或离职时应将经办或保管的档案资料向接办人员交接清楚，不得擅自带走或销毁。

第四条利用好计算机记录和管理，实现房地产档案信息收集、整理、查询、利用管理现代化，提高档案的管理水平和利用质量。利用已建立起来的房地产档案信息库，来进行档案的编目、标引，建立自动检索系统，由计算机辅助进行档案的接收、整理、鉴定、库房管理、借阅利用、统计等。编制完善的检索工具和提高系统的安全防范，做好防病毒工作，抓好用户权限管理。对电子档案要定期进行备份，防止数据损失。

第二章

第一节

第一条文书档案立卷归档法文件资料的收集管理凡公司缮印的公文一律由总经理办公室统一收集保管。

第二条一项工作由几个部门参与办理在工作活动中形成的文件资料，由主办部门收集保管。会议文件由会议召集部门收集整理后交总经理办公室统一收集保管。

第三条公司员工外出培训、学习、考察、调查研究、参加上级机关召开的会议等公务活动在核报差旅费时，必须将有归档价值的文件资料向本部门档案人员办理交接手续，档案员签字认可后会计部才可交予核报差旅费。

第四条各系统部门档案员的职责：

（一）了解本部门的工作业务，掌握本部门的文件资料的归档范

（二）认真执行定期归档制度。对本部门承办的文件资料平时收集归卷，每月的 10 日前应将归档文件资料归档完毕，并向总经理办公室档案员办好交接签收手续。

（三）承办人员借用文件资料时，应积极地做好服务工作，并办理临时借用文件资料登记手续。

第二节 归档范围

第五条重要会议资料，包括会议的通知、报告、决议、总结、领导人讲话、典型发言、会议简报、会议记录、会议纪要、人事档案、工程图纸、技术资料、固定资产清单。

第六条上级机关来的与公司有关的决定、决议、指示、命令、条例、规定、计划等文件资料。

第七条第八条公司对外的正式发文与有关单位来往文书。公司的请示与上级机关的批复；公司反映主要工作活动的报告、总结。

第九条公司内部的各种工作计划、总结、报告、请示、批复、统计报表、重要工作记录（表单）及工作简报。

第十条来人来访及信访工作资料。

第十一条公司于有关单位签订的合同、协议书等文件资料。

第十二条公司管理人员任免的文件资料以及关于员工奖励、处分的文件资料。

第十三条公司的各种规章制度、实施细则、程序文件。

第十四条公司的历史沿革、大事记及反应公司重要活动简报、照片、录音、录像等。

第十五条公司保密制度中规定的保密范围材料。

第三节

第十六条平时归卷各个部门都要建立健全平时归卷制度。对处理完毕或批存的文件资料，由档案管理员集中统一保管。

第十七条各个部门应根据本部门的业务范围及当年工作任务，编制平时文件资料归卷使用的“案卷类目”“案卷类目”的。条款必须简明确切，并标上条款号。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/106143200054010104>