

江苏泰邦认证有限公司

保密控制程序

受控状态：

受控

分 发 号：

编 写： 综合部

审 核： 崔 巍

批 准： 韩树俊

版 本： B/0

2022年12月20日发布

2022年12月20日实施

江苏泰邦认证有限公司发布

1 目的

为规范保密管理工作，维护 TB、获证客户及其相关方的合法权益，确保认证过程中满足法律法规及认可规范要求的保密措施的实施，防止泄密行为的发生。

2 适用范围

本规定适用于公司保密事项全过程的管理。

3 职责

- 3.1 总经理负责中心保密工作的领导与监督实施；
- 3.2 综合部负责办理坐班人员的保密承诺书的签订和日常管理、监督；
- 3.3 市场部负责认证申请、合同文件、资料、信息的保密工作；
- 3.4 审核部负责审核过程中文件、资料、信息的保密工作；
- 3.5 技术部负责认证决定的保密工作，有关申诉/投诉信息的保密工作；
- 3.6 综合部负责专（兼）职审核人员、技术专家专业能力评定、保密承诺书的签订和日常管理、监督；
- 3.7 所有相关部门都有严格遵守公司保密规定的责任和义务。

4 定义

- 4.1 秘密级信息：重要的公司秘密，泄露会使公司的权益和利益遭受损害，包括在研技术信息、经营策略、财务信息等。
- 4.2 一般密级信息：公司一般性决定、决议、通告、通知、行政管理资料、规章制度等。
- 4.3 秘密载体：是指以文字、数据、符号、图形、图像、声音等方式记载企业秘密信息的纸介质、光盘等各类物品，磁介质载体包括计算机硬盘、软盘和录音带、录像带等。
- 4.4 泄密：指使公司秘密被不应知悉者知悉的，或使公司秘密超过了限定的接触范围，使公司秘密信息被泄露。
- 4.5 商业秘密：指不为公众所知悉，能为公司带来经济利益，具有实用性并经公司采取保密措施的技术信息和经营信息。

5 工作程序

5.1 保密范围

5.1.1 遵守国家法律、法规要求的保密信息，未经委托方（或认证客户）同意，不使用或透露其认证方面的信息给任何第三方，但下述情况除外：

- a) TB拥有先于委托方（或认证客户）披露的信息；
- b) 法定的公共信息，或 TB不依赖委托方（或认证客户）获得的信息；
- c) 委托方（或认证客户）已公开的信息；
- d) 认证审核过程的文件、资料、记录；
- e) 应法律法规要求时应公开的信息，如：

- (1) 认证范围;
- (2) 认证基本规范;
- (3) 认证规则;
- (4) 证书有效期;
- (5) 认证收费标准。

5.1.2 已签订的认证合同的有关信息;

5.1.3 从其他来源（如投诉人、监管机构）获得的关于客户的信息;

5.1.4 认证机构的人员，包括代表认证机构工作的任何委员会成员、合同方、外部机构人员或
个人，应对从事认证机构的活动时获得或产生的所有信息;

5.1.5 TB管理、技术等方面的秘密。

5.2 涉密人员管理

5.2.1 本制度中所称的涉密人员是指在工作中产生、掌握、管理和大量接触企业秘密的人员。涉密
人员分为：重要涉密人员和一般涉密人员。

重要涉密人员：在涉及企业秘密岗位上工作或承担任务的人员，可接触秘密级信息载体。本公司重要涉
密人员包括：高层管理人员、技术研发人员、信息上报人员等。

一般涉密人员：在涉及一般密级信息岗位上工作或承担任务的人员，可接触一般密级信息载体。本公
司一般涉密人员包括：主管级管理人员、业务流程岗人员等。

5.2.2 涉密人员定密

涉密人员的涉密等级界定，由各有关部门根据承担工作任务人员的实际涉密情况，提出人员涉密
等级名单，最终由常务副总确定，明确自己应当承担的保密责任、义务。

管理委员会成员、评定部成员、工作人员、专职审核员、兼职审核员、技术专家、分包机构人员均
须严格执行本程序文件的规定，并与TB签订保密及公正性承诺。

5.2 涉密设备管理

5.2.1 各部门应该对本部门可能造成知识产权流失的设备，包括计算机、移动硬盘及其他信
息存储设备、打印机、档案柜等，规定其使用目的、人员和方式。

5.2.2 公司配备的电脑是公司信息处理的主要设备，实行专人管理制度。使用人员应当对自己
的电脑实行加密管理。

5.2.3 公司配备的档案柜钥匙、移动硬盘、U 盘及其他信息存储设备实行登记备案和部
门负责人负责制。

5.3 保密行为规定

5.3.1 委托方（或认证客户）有权提出必要的保密、禁入区等方面要求，并要求审核人员执行保
密承诺;

5.3.2 本机构的管理人员、审核人员、技术专家等均遵守未经申请人书面同意不向第三

方泄露有关信息（应法律要求除外）的规定；如需要向 CNCA、CNAS、CCAA 及同行评审公开保密信息时，应提前告知获证客户；

5.3.3 审核员有对在认证活动过程中所获信息保密的义务，当法律法规要求将信息提供给第三方时，应报告审核部，由审核部按规定程序告知受审核方；

5.3.4 TB各岗位人员不向第三方泄露任何与认证有关的受控文件和信息；

5.3.5 未经同意，不允许任何第三方阅读与 TB和受审核方有关并可作为认证结果的文件。

5.3.6 各有关部门保管的认证企业的有关档案资料，按《文件及记录管理程序》执行。

5.3.7 未经同意，TB的档案室及库房禁止进入，接待客人应到指定房间，各相关部门办公室实行准入原则。

5.3.8 认证机构向其他机构（如 CNAS、同行评审等）公开保密信息时，应将这一行动通知获证客户。

5.4 保密信息的保存及销毁

各部门负责自己部门保密信息及保密文件的保存，需要集中销毁时，移交综合部进行集中销毁。

5.5 泄密事件报告和查处

本程序所称泄密事件是指公司有关部门和个人因违反本程序规定或违反保密承诺内容，使公司秘密被不应知悉者知悉，或者未经允许超出了限定的接触范围而不能证明未被不应知悉者知悉的事件。

5.5.1 泄密事件报告

各部门负责人负责报告本部门发生的泄密事件。各部门发现泄密事件后，应在第一时间上报公司总经理，并立即采取补救措施，积极组织力量查找，以挽回或减少泄密造成的损失。

5.5.2 泄密事件查处

泄密事件查处是指对“泄露公司秘密”事件的调查处理，查处内容包括：

- a) 查明所泄露的秘密事项的内容、密级、危害程度、主要情节和有关责任者；
- b) 积极采取必要的补救措施，防止事态扩大；
- c) 由责任人员负责。并根据情节轻重由管理层提出处理意见，报总经理批准给予纪律处分，直至解聘；
- d) 针对泄密事件暴露出的问题，提出改进和加强保密管理工作的意见；
- e) 因泄密事件引发的法律纠纷，由综合部负责处理。

6 相关支持性文件

TB/CX-T-21 财务控制程序

TB/ZD-T-09 员工手册

7 记录

TB-JT-03-01 保密承诺书

TB-JT-04-11 诚信承诺书

TB-JT-16-13 首次会议签到表及记录

TB-JT-16-14 末次会议签到表及记录