

# T/WJZZ

团 体 标 准

T/WJZZ 015—2024

## 长三角生态绿色一体化发展示范区 智能制造企业商业秘密保护工作规范

Demonstration zone of green and integrated ecological development of the yangtze  
river delta --work specification of trade secret protection for intelligent  
manufacturing enterprises

2024 -2- 1 发布

2024 -2- 1 实施

苏州市吴江区智能制造协会 发布



# 目 次

前言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 基本原则 .....	1
4.1 合法性原则 .....	1
4.2 知悉原则 .....	1
4.3 分割原则 .....	1
5 管理机构和职责 .....	1
5.1 概述 .....	1
5.2 管理机构 .....	2
5.3 管理职责 .....	2
6 商业秘密事项 .....	3
6.1 商业秘密范围 .....	3
6.2 密级 .....	3
6.3 定密 .....	4
6.4 隐密 .....	4
6.5 解密 .....	5
6.6 标识 .....	5
7 保密措施 .....	5
7.1 保密教育 .....	5
7.2 奖惩 .....	5
7.3 人员管理 .....	5
7.4 涉密载体管理 .....	6
7.5 涉密区域管理 .....	7
7.6 商务活动管理 .....	8
7.7 检查和改进 .....	8
8 商业秘密维权 .....	9
8.1 应急处置 .....	9
8.2 证据搜集 .....	9
8.3 技术支持 .....	9
8.4 维权途径 .....	9
附录 A (资料性) 员工保密合同 (参考文本) .....	10
附录 B (资料性) 竞业限制协议书 (参考文本) .....	12
附录 C (资料性) 委托加工保密协议 (参考文本) .....	14

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由苏州市吴江区智能制造协会提出并归口。

本文件起草单位：亨通集团有限公司、康力电梯股份有限公司、上海熊猫机械（集团）有限公司、上海征世科技股份有限公司、日善电脑配件（嘉善）有限公司、苏州迈为科技股份有限公司、苏州恒美电子科技股份有限公司、博众精工科技股份有限公司、苏州绿控传动科技股份有限公司、高创（苏州）电子有限公司、苏州市吴江区市场监督管理局、上海市青浦区市场监督管理局、嘉善县市场监督管理局、长三角生态绿色一体化发展示范区知识产权保护服务中心、嘉善县知识产权保护中心、苏州市吴江区智能制造协会、苏州市吴江区外商投资企业协会。

本文件主要起草人：卫杰、袁春其、王诗璐、孟维龙、丁卫国、陈建兰、蔡晓东、蔡惠祥、蒋琪青、孙喆、郭利华、徐勤锋、沈鸣、任向前、李峰、陶怡灵、周华伟、杜瑞、李芳、曹敬煜、陈萍、郭小川、徐潘芳、宋幽雅、黄海燕、冯晓雯、马琴芳、马振华、严晨曦。

本文件为首次发布。

# 长三角生态绿色一体化发展示范区 智能制造企业商业秘密保护工作规范

## 1 范围

本文件规定了企业商业秘密管理规范的术语和定义、基本原则、管理机构和职责、商业秘密事项、保密措施、商业秘密维权。

本文件适用于长三角生态绿色一体化发展示范区智能制造企业商业秘密保护管理，其它企业可参考执行。

## 2 规范性引用文件

本文件没有规范性引用文件。

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

#### 智能制造企业 Intelligent Manufacturing Enterprises

智能制造企业定义为基于新一代信息技术，贯穿设计、生产、管理、服务等制造活动各个环节，具有信息深度自感知、智慧优化自决策、精准控制自执行等功能的先进制造过程、系统与模式的企业。

### 3.2

#### 商业秘密 Trade Secrets

不为公众所知悉，具有商业价值并经权利人采取相应保密措施的技术信息和经营信息等商业信息。

### 3.3

#### 涉密载体 Classified Carriers

以文字、数据、符号、图形、图像、视频和音频等方式记录商业秘密信息的各类物质，如纸质文件、存储介质（终端：电脑、打印机等；移动存储终端：U盘、手机等；私有/公有云存储等）和其他介质。

## 4 基本原则

### 4.1 合法性原则

商业秘密管理应遵守国家法律、法规、规章、司法解释及规范性文件等规定。

### 4.2 知悉原则

根据管理、科研、业务工作的需要，若不向员工授权掌握某项商业秘密就无法进行生产、工作或者达成某项交易，应使其知悉的内容。

### 4.3 分割原则

把完整的事项根据经营、管理不同环节分割成若干部分，每个环节只能知悉本部分商业秘密的内容。

## 5 管理机构和职责

### 5.1 概述

商业秘密管理工作实行统一领导、分级管理、分工负责的领导体制和工作机制。

## 5.2 管理机构

### 5.2.1 企业保密委员会

企业保密委员会是企业商业秘密管理的最高组织机构，委员会设主任、副主任，主任宜由企业主要负责人担任，副主任由企业各部门负责人担任。主要工作职责包括：

- a) 审定企业商业秘密工作部署及年度工作安排；
- b) 提供企业商业秘密保护体系相关资源，支持和推动商业秘密管理工作的实施；
- c) 评审与监督企业商业秘密工作有关的重大事项。

### 5.2.2 企业商业秘密管理办公室

企业商业秘密管理办公室是在企业保密委员会领导下，具体负责商业秘密的归口管理部门，推荐知识产权管理部门或法务风控管理部门负责，其主要职责：

- a) 宣传贯彻国家保密法规和企业有关保密制度；
- b) 组织制定企业商业秘密保护规章制度并监督执行；
- c) 制定企业商业秘密年度工作计划并按期推进；
- d) 负责企业商业秘密工作日常管理；
- e) 调查处理企业失、泄、窃密事件。

### 5.2.3 企业人力资源部门

5.2.3.1 企业人力资源部门负责开展新员工入职培训，将商业秘密的管理纳入培训内容，并详细说明部门及岗位的涉密内容、管理制度。

5.2.3.2 开展新员工入职背景调查，对签订同行业《竞业限制协议》和保密合同的人员在限定期限届满前，不建议招聘。

5.2.3.3 负责公司人力资源相关商业秘密管理。

5.2.3.4 负责对离职人员进行定期评估履行竞业限制等情况。

### 5.2.4 企业信息技术部门

企业信息技术部门负责企业涉密网络、信息系统、计算机和移动存储介质的保密管理工作，落实计算机信息网络的安全保密工作。

### 5.2.5 企业各部门和商业秘密管理人员

#### 5.2.5.1 部门负责人

企业各部门负责人为商业秘密保护的第一责任人，负责确定和修改部门商业秘密的事项和范围，并实施有效的管理。

#### 5.2.5.2 专(兼)职保密员

涉密部门应设立专(兼)职保密员岗位，其职责包括：

- a) 宣传商业秘密保护的意義、作用，增强全员的保密意识；
- b) 按照国家及企业各项保密规定，推进落实各项保密事项；
- c) 监督检查本部门保密工作，发现问题及时整改；
- d) 拟定本部门商业秘密的定密、解密方案，并予以落实；
- e) 协助调查处理本部门失、泄、窃密事件。

## 5.3 管理职责

### 5.3.1 领导负责制

企业对商业秘密的保护实行领导负责制。

### 5.3.2 分工负责制

- 5.3.2.1 企业对商业秘密的保护实行分工负责制，遵循“谁主管，谁负责”和“谁涉密，谁负责”的原则。
- 5.3.2.2 企业分管保密工作的领导担负具体组织领导的责任，分管有关方面工作的领导负责分管工作范围内的保密工作。
- 5.3.2.3 企业各部门负责各自职责范围内涉密事项的保密管理、监督和检查工作，并针对本部门实际业务工作制定专业性保密管理措施。

## 6 商业秘密事项

### 6.1 商业秘密范围

- 6.1.1 技术类涉密信息保护范围参见表1。

表1 技术类涉密信息

类别	表现形式
设计信息	设计图及其草案、模型、样机、设计方案、测试记录及数据等。
采购技术信息	型号、牌号、定制品技术参数、特别要求等。
生产信息	产品的配方、工艺流程、技术参数、电子数据、作业指导书等。
设备信息	生产设备、仪器、夹具、模具等中的技术信息。
软件程序	设计计划、设计方案、源代码、应用程序、电子数据等。
其他	企业认为有必要采取保密措施的其他技术信息，如未公开的专利申请信息等。

- 6.1.2 经营类涉密信息保护范围参见表2。

表2 经营类涉密信息

类别	表现形式
管理文件	文件、规章制度等。
决策信息	战略决策、管理方法、项目投资策略及方案等。
研发信息	研发策略、研发经费预算等。
采购信息	供应商信息、竞价策略、采购渠道、主要原材料指标、采购计划、采购记录、采购价格等。
销售信息	营销计划、营销方案、营销政策、营销手册、销售协议、销售记录、销售价格等。
招投标信息	标书、标底等。
财务信息	财务报表、财务分析、统计报表、预决算报告、各类帐册、银行存款核算、外部会计报告、内部会计报告、股权调整方案等。
供应商和客户信息	名称、联系人、联系方式、交易习惯、合同内容、交提货方式、款项结算等。
人力资源信息	企业人力资源计划、人力资源结构、薪酬方案、员工档案、员工名册、职位、联系方式等。
运营信息	企业改革和发展方案、技术合作方案、突发事件处置方案、涉稳事件处置方案、突发和涉稳事件处置资料、产能信息、生产计划等。
其他	企业认为有必要采取保密措施的其他经营信息。

### 6.2 密级

企业商业秘密按重要程度以及泄露后会使企业利益遭受损害的程度，分为：关键性商密、重要性商密、一般性商密或一级商密、二级商密、三级商密，共三个等级（具体以企业自身实际情况而定义）。

具体包括：

- a) 关键性商密或一级商密：指具有最高敏感性的信息，如果泄露或者不当使用，将会使企业利益遭受重大损失或产生严重影响。
- b) 重要性商密或二级商密：指对组织关键的信息，如果泄露或者不当使用，将会使企业利益遭受一定的损失或产生不良影响。
- c) 一般性商密或三级商密：指对组织有影响的信息，如果泄露或者不当使用，可能会使企业利益遭受损害或产生影响。

### 6.3 定密

#### 6.3.1 定密评估

定密时应从表3的因素考虑泄密后产生的影响。

表3 涉密影响

序号	因素	影响
1	商业价值	现在的和将来的
2	损失	可能造成的损失程度
3	竞争企业	对竞争企业产生的价值
4	合同或法律法规	违反后的法律责任

#### 6.3.2 商业秘密项目的确定程序

##### 6.3.2.1 保密期限：

- a) 企业应结合密级分级、市场需求、技术成熟度、发展规划等情况，确定各商业秘密的保密期限；
- b) 可以预见具体保密期限的，以年、月、日计，不可预见的应定为“长期”或者“公开前”。

6.3.2.2 商业秘密产生部门拟定保密项目，建议保密期限和知悉范围，本部门保密员审核、本部门主要负责人签批确认后，报至企业商业秘密管理办公室。

6.3.2.3 商业秘密管理办公室牵头相关部门、人员对提出的商业秘密确认申请进行论证，并给出论证结果。

6.3.2.4 商业秘密管理办公室根据企业规定对审批后的密级文件确认保密期限、知悉范围等，报送企业保密委员会审批后执行。

#### 6.3.3 商业秘密项目变更

6.3.3.1 密级和保密期限确定后，发现下列情形之一的，应及时变更：

- a) 泄露后对企业利益的损害程度发生明显变化的；
- b) 因工作需要，原知悉范围有较大变化的；
- c) 事项密级或保密期限已经发生变化的。

6.3.3.2 变更流程如下：

- a) 涉及商业秘密的部门提出商业秘密变更和解除申请；
- b) 商业秘密管理办公室组织对商业秘密进行评估；
- c) 商业秘密管理办公室根据评估结果，出具商业秘密变更、解除意见；
- d) 企业保密委员会对变更和解除进行确认审批；
- e) 商业秘密管理办公室根据审批的情况，重新确定商业秘密管理台账的状态；
- f) 密级、保密期限变更后，涉及商业秘密部门应及时变更标识。

### 6.4 隐密

6.4.1 企业在对外公开发布信息或与供应商、客户、合作方、其他单位沟通时应注意隐密，可对涉密信息进行模糊化技术处理以便隐藏，或者删除涉密信息：

- a) 与供应商、客户、合作方等的沟通和信息往来中；
  - b) 信息公开、发布、流转时；
  - c) 协助其他单位尽职调查时；
  - d) 其他情形。
- 6.4.2 配合行政机关和部门的行政检查、行政执法中，涉及隐密事项检查的，企业应主动提醒执法检查人员履行保密义务。
- 6.4.3 可采取的隐密方式为：
- a) 隐藏或删除涉密信息；
  - b) 对涉密信息进行模糊化处理；
  - c) 其他方式。

## 6.5 解密

当保密期限已满，评估商业秘密事项已不再具有保护价值的，或者因特定因素导致商业秘密被公开的应予解密。解密需要对实物和电子版同时消除或涂改密级标识，并移出涉密区域。

## 6.6 标识

涉密信息的密级和保密期限一经确定，不得随意变更，并在涉密信息载体的显著位置进行标注。

## 7 保密措施

### 7.1 保密教育

- 7.1.1 商业秘密保护教育应列入企业年度培训计划，促使在职员工对商业秘密可能泄露的异常状态及承担法律后果保持足够警觉。
- 7.1.2 企业商业秘密管理办公室组织对中层领导及各部门保密员开展培训教育，再由各部门进行内部培训，采用横向纵向相结合的方法，达到全员保密教育，增强保密意识。
- 7.1.3 保密教育可以采用多种形式，并对结果进行考核，使全体员工自觉遵守保密基本准则。

### 7.2 奖惩

- 7.2.1 对员工依照企业规定，在保守企业秘密方面，能忠于职守，从事保密工作取得显著成效的；发现他人泄密，能立即采取补救措施，避免或减轻损害后果的；对泄密或者非法获取企业秘密的行为及时检举的，按照有关规定给予奖励。
- 7.2.2 对员工因不遵守企业规定，造成泄密事件，依照有关法规及企业的奖惩制度，给予纪律处分、解雇，直至追究其法律责任。

### 7.3 人员管理

#### 7.3.1 招聘管理

- 7.3.1.1 对涉密重点岗位员工入职前宜做背景调查。
- 7.3.1.2 不应以取得第三方的商业秘密为目的录用竞争性企业的员工。
- 7.3.1.3 在录用竞争性企业的员工时，宜审核其与原单位之间的保密内容及期限，提醒不应将原单位的商业秘密带入本企业内部进行使用或公开，并要求签署保证书。

#### 7.3.2 入职管理

- 7.3.2.1 新入职或转岗到涉密岗位的员工，应与其签订员工保密合同(参见附录A)。
- 7.3.2.2 高级管理人员、高级技术人员及其他负有保密义务的人员可在企业评估后与其签订竞业限制协议(参见附录B)。
- 7.3.2.3 应对新入职人员进行保密培训，培训结束后宜进行考核，并保存培训和考核记录。

#### 7.3.3 履职管理

- 7.3.3.1 员工应遵守企业商业秘密保护制度，做好本岗位商业秘密保护工作：

- a) 按企业的授权权限查阅使用涉密信息；
- b) 按企业规定使用办公电脑并妥善保管商业秘密载体；
- c) 不登录未授权的账户和系统；
- d) 不进入非授权涉密区域。

7.3.3.2 宜对中高层管理人员和涉密重要岗位员工的下列行为进行限制：

- a) 兼职、入股、组建、参与组建或变相投资与所在企业经营相类似的企业；
- b) 同上述企业进行交易；
- c) 同与所在企业有竞争关系的企业进行涉密交易。

#### 7.3.4 离职管理

7.3.4.1 在涉密岗位员工离职时，企业应主动告知保密义务，以及若违反规定应承担的相应法律责任，并告知离职员工不应有以下行为：

- a) 复制、带离、损毁、篡改、拍摄涉密文件资料、物品；
- b) 查阅、拷贝、篡改、拍摄涉密文件资料、物品；
- c) 删除、更改账户；
- d) 披露、使用商业秘密等。

7.3.4.2 提醒离职员工主动移交一切涉密载体和物品：

- a) 涉密文件资料、数据及其载体、物品；
- b) 账号、秘密等账户信息；
- c) 工作电脑；
- d) 门禁卡、钥匙等。

7.3.4.3 宜对其采取适当措施进行脱密，应及时回收注销离职员工的办公、网络、门禁等系统权限，并及时通知与离职员工有关的供应商、客户、合作单位等，做好业务交接。

7.3.4.4 评估是否需要履行竞业限制协议或与其重新签署竞业限制协议；对需要履行竞业限制义务的人员定期掌握其在竞业限制期内的任职去向。

### 7.4 涉密载体管理

#### 7.4.1 纸质文档

##### 7.4.1.1 保管

涉密纸质文档应由专人保管，存放于指定地点，建立健全商业秘密载体的收发登记、签收、催办、清退、借阅、归档制度，由部门保密员登记造册，按权限使用、查阅、借阅、续借并履行登记手续。管理人员离职前，应办理移交手续。

##### 7.4.1.2 使用

7.4.1.2.1 打印、复印、扫描、传真、查阅、借阅、向第三人披露或提供时，应按权限或通过审批使用，并履行登记手续，复印件与原件的密级和保密期限相同。

7.4.1.2.2 制作商业秘密载体，应当进行定密、标密，建立台账，在发放时应严格按批准的范围执行，并做好发放登记管理；制作过程应进行保密，落实专人负责制作、收转、存档。涉密载体原则上应在本单位制作，委托外单位制作应事前签订保密协议或在合同条款中约定保密事项及违约后应承担的责任，制作过程中形成的校样、印版、底片和废品等，应及时专人监督销毁。

7.4.1.2.3 收到商业秘密载体，应履行清点、签收等手续，并建立登记台账。

7.4.1.2.4 不得通过普通传真机、公用电子邮件、手机短信、聊天工具、普通邮政传递商业秘密载体。企业部门之间传递商业秘密载体应使用专业办公软件或专人密封报送。

7.4.1.2.5 关键性商密（或一级商密）、重要性商密（或二级商密）和文件、资料除知悉范围人员外，员工查阅须经企业商业秘密管理办公室或企业保密委员会批准，但不得借出。

7.4.1.2.6 严禁复制关键性商密（或一级商密）秘密载体。复制重要性商密（或二级商密）以下商业秘密载体，应由本部门负责人审核，经企业商业秘密管理办公室批准，复制件视同原件进行登记管理；汇编涉密文件、资料，应经商业秘密产生部门许可，汇编成册的文件、资料，应按其中最高密级和最长保密期限进行密级文件管理。

### 7.4.1.3 销毁

销毁纸质的商业秘密，须由商业秘密管理办公室审核，经企业保密委员会批准，履行登记手续后，在保密办指定的场所按规定的方法进行，并在专人监督下销毁。应做好销毁人员、时间、数量、方式等信息的留存。

## 7.4.2 电子信息

### 7.4.2.1 存储

涉密电子信息应采用加密方式存储于企业授权的存储设备、应用系统或云存储空间，并定期备份。

### 7.4.2.2 流转

涉密电子信息的收发应使用唯一出入口，对涉密数据流入流出进行审批，宜采取下列管理措施：

- a) 内部局域网应与互联网隔离，涉密数据网络传递应通过内部局域网或加密网络通道对外传输；
- b) 通过邮件发送涉密数据时，应设置加密和签名，限定文档的读写权限、打开次数和时限；
- c) 指定专人进行解密操作；
- d) 应与客户、合作单位等涉密数据接手单位或个人签订保密协议；
- e) 文档首页、页眉、页脚、页面水印等设置保密义务提醒。

### 7.4.2.3 权限管理

7.4.2.3.1 企业应对计算机控制 USB 接口、外网、设备、数据库和各类应用系统及其账户实行权限管理，按岗位职责或特定工作事项以“最小够用”原则设定权限：

- a) 合理分配不同层级账户的功能和审批权限；
- b) 合理分配项目中不同账户的功能和使用期限；
- a) 合理设定不同账户的访问、操作、查看等权限及其使用期限；
- b) 合理设定不同账户的互联网使用权限等。

7.4.2.3.2 权限到期、人员转岗、项目或事项变更时应重新授权；

7.4.2.3.3 人员离职时应回收相应权限。

### 7.4.2.4 口令管理

7.4.2.4.1 各类数据库和应用系统应设账户和密码。

7.4.2.4.2 密码通常应包含数字和字母且不少于 8 位的中等复杂程度密码，禁止使用默认密码、出生日期或 123456 等简单密码或保存自动字符，并按规定时间间隔进行密码更改。

7.4.2.4.3 宜对所有涉密账号和密码实行统一登记、备案、发放和变更管理。

### 7.4.2.5 存储介质

#### 7.4.2.5.1 计算机

7.4.2.5.1.1 涉密计算机应关闭或禁用移动存储、光驱、蓝牙、无线网卡等数据传输功能，以及摄像头、声卡、话筒等音视频采集功能。

7.4.2.5.1.2 涉密计算机的配置、维修、报废均应经过审批或授权交由指定人员处理，禁止员工私自拆机维修、更换、增加配件。

7.4.2.5.1.3 计算机未经审批不应安装非授权软件，不得接入非授权网络。

#### 7.4.2.5.2 移动存储介质

7.4.2.5.2.1 移动存储设备应经审批后存储商业秘密信息。

7.4.2.5.2.2 涉密移动存储介质应由专人专管，并采取内容加密、设备绑定等保密措施，不应连接非涉密或未采取保密措施的计算机或电子设备。

## 7.5 涉密区域管理

### 7.5.1 涉密区域识别

宜将下列部门或地点列为涉密重点区域：

- a) 研发设计环节中的实验室、研发部门核心区域、未公开试验样品存放地等区域；
- b) 采购环节中的原材料、半成品等涉密物资存放区域；
- c) 控制中心、重要生产场所、服务器机房等；
- d) 其他涉密区域，包括知识产权、信息管理、财务、人力资源、销售、商务等重点部门的办公场所，以及涉密档案和载体的存放区域等。

## 7.5.2 安防措施设置

7.5.2.1 涉密区域入口处应设置门禁，安装监控视频和报警装置，张贴标识和警示语。应采取物理措施将涉密区域与非涉密区域进行隔离。

7.5.2.2 限制使用具有录音、摄影、摄像、信息存储等功能的设备。

7.5.2.3 涉密区域限制外来人员访问、参观、考察，确因工作需要进入的应履行审批手续并全程监督。

## 7.5.3 网络安全措施

企业涉密区域的涉密网络可采取如下保密措施：

- a) 不应接入外网；
- b) 与内部网络隔离，不能相互连通；
- c) 通过 VPN 等方式远程接入涉密区域网络应使用终端准入、权限审批等。

## 7.6 商务活动管理

### 7.6.1 人员出入管理

企业宜采取如下措施加强涉密区域人员出入管理：

- a) 内部人员出入应具备相应权限，佩戴身份标识卡，非授权人员应经审批获得临时授权方可进入；
- b) 外部人员访问涉密区域应经审批，履行出入登记手续，佩戴临时证件，由专人全程陪同；
- c) 对出入人员限制其使用具备录音、拍照、摄像、存储功能的设备。

### 7.6.2 涉密会议或活动

7.6.2.1 涉及商业秘密的会议或宣传推广活动，应采取以下保密措施：

- a) 选择具有保密条件的场所，与场所提供方签订保密协议；
- b) 限定参加人员范围，指定参与涉密事项人员；
- c) 告知保密要求，必要时签订保密承诺书；
- d) 涉密文件资料应有明显保密和会后回收标识，休会或会议结束时，及时收回清点、登记；
- e) 通过摄影、摄像、签名等方式，做好记录。

7.6.2.2 商务、技术合作与委托生产，应采取以下保密措施：

- a) 商务技术合作、共同研究及涉及商业秘密的交易活动时，应签订保密合同。书面明确利用合作方或己方提供的秘密信息开发成果的所有权与使用权，防止本企业自行研究、开发活动中带入合作方秘密信息。
- b) 聘任或委托的外聘专家、顾问、翻译、律师等可能接触涉密信息的外部人员，宜做背景调查，并签订保密协议。
- c) 在收购技术和客户名单等经营信息时，通过尽职调查、合同条款约束等方式确保出售方对出售标的享有充分有效的处置权。

7.6.3 涉及商业秘密的委托加工，应与加工方签订保密协议(参考附录 C)。

## 7.7 检查和改进

7.7.1 应进行年度定期检查和不定期抽查，检查内容如下：

- a) 商业秘密保护规章制度建立和实施情况；
- b) 涉密人员培训、管理等情况；
- c) 涉密区域管理情况；
- d) 涉密信息传输情况；

- e) 涉密文件资料的管理情况;
  - f) 涉密载体、物品的管理情况;
  - g) 商业秘密事项的定密、隐密、解密情况。
- 7.7.2 发现有泄密情况及隐患的,应及时纠正。

## 8 商业秘密维权

### 8.1 应急处置

- 8.1.1 参照附录D制定商业秘密泄密紧急处理预案,建立泄密事件紧急应对流程。
- 8.1.2 当发现有泄密迹象时,启动应对流程,防止进一步扩散和损失进一步扩大,将危害控制在最小限内。

### 8.2 证据搜集

发现商业秘密涉嫌被侵权时,应搜集并整理以下证据性材料并及时进行证据保全:

- a) 侵权主体信息;
- b) 侵犯涉密信息的具体行为表现;
- c) 侵权后果,即侵权行为导致本企业的损失情况,及可能导致的后果;
- d) 可能与泄密信息有关的人员情况(单位、保密合同/协议、工作经历、社会关系);
- e) 泄密信息的具体内容、载体、途径;
- f) 企业已采取的保护措施;
- g) 泄密信息具有现实或潜在的商业价值;
- h) 泄密信息的权属。

### 8.3 技术支持

- 8.3.1 可向商业秘密保护服务机构寻求帮助。
- 8.3.2 可向专业机构申请涉密信息的非公知性、同一性、价值性鉴定。

### 8.4 维权途径

根据证据收集情况,企业可依法采取下列方式进行维权:

- a) 请求调解组织进行调解;
- b) 向市场监督管理部门举报;
- c) 涉及劳动关系的可向劳动仲裁机构申请仲裁;
- d) 根据仲裁条款或达成的仲裁协议提请仲裁机构仲裁;
- e) 涉嫌犯罪的可向公安机关举报、控告;
- f) 向人民法院提起诉讼;
- g) 向人民检察院申请对商业秘密司法活动进行监督。

附 录 A  
(资料性)  
员工保密合同 (参考文本)

甲方：  
联系电话：  
乙方：  
性别：  
身份证件号码：  
户籍地址：  
通讯地址：  
联系方式：

甲乙双方就乙方在任职期间及离职以后的保密及竞业限制事宜，达成以下条款，以共同遵守：

一、商业秘密信息

1、甲乙双方确认：“商业秘密”是指甲方及其关联企业不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息等，甲方企业中列为关键性商密（或一级商密）、重要性商密（或二级商密）、一般性商密（或三级商密），包括但不限于设计、程序、制作工艺、制作方法、管理措施、产品或服务的销售网络、销售状况、客户名单、市场开发及售后服务情况、产销策略、招投标中的标底及标书内容。

2、乙方承认在为甲方工作期间可能直接或间接地通过书面、口头、图表、音像资料等获得或通过观察全部或部分设备、产品等获得这些秘密信息。

3、甲乙双方同意，上述“秘密信息”不包含非因乙方过错而进入公众领域的公开信息。

二、对商业秘密信息的保密

1、乙方承诺，严格保守自己在为甲方工作期间所获得有关甲方及甲方项目的一切秘密信息。

2、乙方保证除非为了甲方项目的工作需要交流此种秘密信息外，未经甲方事先书面许可，不以任何方式，无论口头、书面，还是U盘、通信网络等介质向任何其他方，包括个人、企业、商社、其他经济组织等泄露秘密信息。

三、禁止非法使用商业秘密信息

乙方保证除非为了甲方项目的工作需要而使用此种商业秘密信息履行职务外，未经甲方事先书面许可，不以任何方式自行使用商业秘密信息，并且不以任何方式许可或协助他人使用商业秘密信息。

四、商业秘密信息的停止使用

1、在甲、乙双方劳动关系无论何种原因终止或解除后，乙方应停止使用所有的商业秘密信息，而且只要此种商业秘密信息尚未依法进入公众领域，乙方就不得继续使用，也不得向任何个人、企业、商社、其他经济组织等披露此种商业秘密信息。

2、在甲、乙双方的劳动关系存续期间及终止或解除后，一旦甲方要求，乙方应随时将从甲方及甲方项目获得的一切资料文件及其复制件归还甲方或进行销毁。

五、保密期限

1、双方同意本协议规定的保密期限为自本协议签署之日起至双方劳动关系终止或解除后\_\_年内有效。

2、在保密期限内，乙方无论因何种原因从甲方或甲方关联企业离职，仍须承担如同任职期间一样的保密义务；乙方认可，甲方及甲方关联企业在支付工资报酬时，已考虑了乙方离职后需要承担的保密义务，故而无需在乙方离职时另外支付保密费。

六、违约责任

1、如果乙方违反本协议的规定，应赔偿甲方全部损失。赔偿范围包括但不限于甲方的名誉损失、直接损失和可得利益的损失，以及调查费用和诉讼费用、律师费用。

2、乙方违约后还应采取各种合理方法挽回泄密造成的影响，尽可能使商业秘密信息继续处于保密状态。同时，本协议继续有效。

3、乙方违反本协议任何条款的行为均视为严重违反劳动纪律和甲方规章制度，无论违约金及损失赔偿金给付与否，甲方均有权不经预告立即解除与甲方的聘用关系。

七、协议的生效与效力

1、本协议自甲、乙双方签字之日起生效。本协议一式二份，甲、乙双方各执一份，具有同等法律效力。

2、双方就履行中产生的任何争议，应通过友好协商解决，协商不成，任何一方有权向人民法院提起诉讼。

甲方(盖章):

乙方(签字):

签订日期:       年   月   日

**附 录 B**  
**(资料性)**  
**竞业限制协议书 (参考文本)**

甲方(用人单位):

乙方(劳动者): 身份证号:

乙方已同甲方签订劳动合同,且为甲方员工,因工作需要,接触到甲方的商业秘密,为保护甲方的商业秘密及其合法权益,确保乙方在职期间和离职后不与甲方竞业,甲、乙双方根据《中华人民共和国劳动合同法》等法律法规,在遵循平等自愿、协商一致、诚实信用的原则下,就乙方对甲方承担的竞业限制义务及甲方因乙方承担竞业限制义务而对乙方的补偿等相关事项达成如下协议:

一、未经甲方同意,乙方在任职期间不得从事以下行为:

- 1、自己开业生产或经营与甲方生产或经营产品同类的产品;
- 2、自营与甲方同类的业务;
- 3、为他人经营与甲方生产或经营的产品同类的产品;
- 4、为他人经营与甲方同类的业务。

二、乙方离职后的竞业禁止义务

1、不论因何种原因从甲方离职,乙方应立即向甲方移交所有自己掌握的,甲方企业中列为关键性商业秘密(或一级商业秘密)、重要商业秘密(或二级商业秘密)、一般性商业秘密(或三级商业秘密),包含有职务开发中商业秘密的所有文件、记录、信息、资料、器具、数据、笔记、报告、计划、目录、来往信函、说明、图样、蓝图及纲要(包括但不限于上述内容之任何形式之复制品),并办妥有关手续,所有记录均为甲方绝对的财产,乙方将保证有关信息不外泄,不得以任何形式留存甲方有关商业秘密信息,也不能以任何方式再现、复制或传递给任何人,更不得利用前述信息谋取利益。

2、不论因何种原因从甲方离职,离职后\_\_年(不超过二年)内,不得到\_\_\_\_\_ (具体竞业限制区域)参与甲方从事的行业相同或相近的企业,及与甲方有竞争关系的企业内工作。

3、不论因何种原因从甲方离职,离职后\_\_年(不超过二年)内,不得到\_\_\_\_\_ (具体竞业限制区域)自办与甲方有竞争关系的企业或者从事与甲方商业秘密有关的产品的生产。

4、在与甲方离职后\_\_年(不超过二年)内,不得到\_\_\_\_\_ (具体竞业限制区域)直接地或间接地通过任何手段为自己、他人或任何实体的利益或与他人或实体联合,以拉拢、引诱、招用或鼓动之手段使甲方其他成员离职或挖走甲方其他成员,不得劝说、诱使、抢夺甲方客户或潜在客户。

5、从乙方离职后开始计算竞业限制期,甲方向乙方支付补偿费,在竞业限制期间甲方给予乙方不低于其任职期间月均工资(包括年终奖的一切劳动报酬)的\_\_\_%标准支付津贴作为补偿。

6、竞业禁止期满,甲方即停止补偿费的支付。

三、违约责任

1、乙方不履行规定义务的,违反本合同任一条款,给甲方造成损失的,应当承担违约责任,乙方应当支付甲方违约金人民币\_\_\_\_\_元,并承担甲方由此引起的一切损失。损失无法计算时,最低赔偿甲方人民币\_\_\_\_\_元计算,如违约金不足赔偿甲方损失的,甲方还有全向乙方主张由此遭受的经济损失。

2、甲方不履行规定义务的,应当依照法律规定承担违约责任。

四、争议解决

因履行本协议发生的劳动争议,双方应以协商为主,如果无法协商解决,争议一方或双方有权向甲方所在地的劳动争议仲裁委员会申请仲裁。

五、其他

1、本协议提及的技术秘密,包括但不限于:技术方案、工程设计、产品设计、制造方法、产品材料构成、工艺流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、实验数据、试验结果、图纸、样品、样机、模型、模具、操作手册、技术文档、相关的函电等等。

2、本协议提及的商业秘密,包括但不限于:客户名单、行销计划、采购资料、定价政策、财务资料、进货渠道等。

3、本协议未尽事宜，或与今后国家有关规定相悖的，按有关规定执行。

4、本协议及甲乙双方所签订的《保密协议》作为劳动合同附件，经甲乙双方签字盖章后，具有同等法律效力。

5、一式两份，甲乙双方各持一份，具有同等法律效力。

甲方：

地址：

法定代表人：

签署人签字：

电话：

乙方(员工) (签字)：

住址：

职务：

电话：

身份证号码：

附 录 C  
(资料性)  
委托加工保密协议 (参考文本)

甲方 (委托方):

住址:

法定代表人:

乙方 (加工方):

住址:

法定代表人:

乙方与甲方基于委托加工 (开发), 已经 (或将要) 知悉甲方的商业秘密。甲、乙双方平等协商, 依据中国有关法律法规订立本保密协议。双方确认在签署本协议前, 已经详细审阅过协议的内容, 并完全了解协议各条款的法律含义。

一、保密的内容和范围

1、甲、乙双方确认, 乙方应承担保密义务的甲方商业秘密范围包括但不限于以下内容: 1、技术信息。技术信息的范围一般包括技术方案、工程设计、电路设计、制造方法、配方、工艺流程、技术指标、计算机软件、数据库、试验结果、图纸、样品样机、模型模具、操作手册、技术文档、涉及商业秘密的业务函电等。

2、经营信息。经营信息的范围一般包括客户名单、营销计划、采购资料、定价政策、不公开的财务资料、劳动报酬、进货渠道、产销政策、招投标中的标的及标书内容等。

3、公司依照法律规定和有关协议约定对外应承担保密义务的事项等。

二、乙方的保密义务

1、主动采取加密措施对上述所列及之商业秘密进行保护, 防止不承担同等保密义务的任何第三方知悉及使用;

2、不得刺探或者以其他不正当手段 (包括利用计算机进行检索、浏览、复制等) 获取与本职工作或本身业务无关的甲方单位的商业秘密;

3、不得向不承担同等保密义务的任何第三人披露甲方单位的商业秘密;

4、不得允许 (包括出借、赠与、出租、转让等行为) 或协助不承担同等保密义务的任何第三人使用甲方单位的商业秘密;

5、不论因何种原因终止与甲方单位的委托关系, 都不得利用甲方单位的商业秘密为其他与甲方有竞争关系的企业 (包括自办企业) 服务;

6、甲方单位商业秘密所有权始终全部归属甲方, 乙方不得利用自身对甲方单位的商业秘密不同程度的了解申请对于甲方单位的商业秘密所有权, 在本协议签订前经乙方书面证明已依法具有某些所有者除外;

7、如发现甲方关于甲方单位的商业秘密被泄露或者自己过失泄露秘密, 应当采取有效措施防止泄密进一步扩大, 并及时向甲方公司报告。

三、商业秘密的停止使用

1、在甲、乙双方委托关系无论何种原因终止或解除后, 乙方应停止使用所有的甲方商业秘密, 而且只要此种商业秘密尚未依法进入公众领域, 乙方就不得继续使用, 也不得向任何个人、法人或其他经济组织等披露此种商业秘密。

2、在甲、乙双方的委托关系存续期间及终止或解除后, 一旦甲方要求, 乙方应随时将从甲方及甲方项目获得的一切资料文件及其复制件归还甲方或双方销毁。

四、保密期限

双方同意本协议规定的保密期限为自本协议签署之日起至双方合作关系终止或解除后二年内有效。

五、违约责任

如果乙方不履行本协议所规定的保密义务, 应当承担违约责任。如果因为乙方的违约行为造成甲方的损失, 应当承担下列责任:

1、包括但不限于赔偿甲方的一切损失和额外费用支出：甲方支付的全部诉讼费用、律师费用、为处理此事所产生的其他费用、甲方因此所导致遭第三方的索赔费用和承担违约赔偿费用、甲方其他相关经济损失等。

2、给甲方造成不良社会影响和商业信誉影响的，乙方还应当配合甲方消除不良影响，协助甲方追查、追回因乙方违约行为所流出的属于甲方的技术资料和商业信息或所有由甲方提供给乙方的技术资料和商业信息资料、产品及产品零配件等。无法消除不良影响的，或者无法追回、追查的，或者追回前甲方已经遭受损失的，甲方有权按本条第一项（1）条约定内容处理。

#### 六、争议的解决办法

因执行本协议而发生纠纷，双方协商解决，协商不成，任何一方均应向甲方所在地人民法院提起诉讼。

#### 七、协议的效力和变更

本协议自双方签字盖章后生效，之前签订的其他协议与本协议冲突的，以本协议为准。（以下无正文，为各方签字页）

甲方（签章）：

乙方（签名）：

---