ICS 03.100.01
CCS A 01

DB46

# 海 南 省 地 方 标 准

DB46/T 584—2023

# 商业秘密保护管理规范

Management specifications for protection of trade secrets

2023-05-29 发布　　2023-07-01 实施

海南省市场监督管理局　　发 布

# 目　　次

# 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。

本文件由海南省市场监督管理局提出并归口。

本文件起草单位：海南省质量技术监督标准与信息所、海南省标准化协会。

本文件主要起草人：李伟、吴清宇、王小英、孙林芳、汤雪、黄家将、梅姬、金佳佳、李廷秀。

# 引　言

商业秘密是市场经济发展的产物，是知识产权的重要组成部分，也是企业重要的无形资产，它对企业在市场竞争中的生存和发展有着重要影响。我国自加入世贸组织以来，对外开放经济活动已逐渐与国际接轨，保密环境日趋复杂，商业秘密越来越容易受到侵害。在市场经济条件下，进一步加强企业商业秘密保护工作，对于保护企业知识产权，提高企业管理水平，增强企业竞争能力，促进企业进一步发展十分重要。

近年来，部分企业已经认识到保护商业秘密的重要性，建立了相应的商业秘密保护制度，取得了一定的效果，但是从总体上看，我省多数企业保护商业秘密的意识仍然比较淡薄，保护措施依然比较落后，致使侵害企业商业秘密权益的案件不断增加，企业商业秘密被泄密和窃取的现象屡有发生，企业的生产经营受到了严重影响。

为了创建海南自由贸易港一流的营商环境和公平竞争市场秩序，增强企业商业秘密保护意识，规范和推动企业商业秘密保护管理工作，提升企业对泄密风险的管控能力和应急水平，优化公平竞争的营商环境，根据国家市场监管总局的要求，结合我省实际，制定本标准。

本文件引导企业开展商业秘密保护工作，强化公平竞争意识，自觉依法合规经营，减少商业秘密泄露风险，同时也避免侵犯他人商业秘密；为创建海南自由贸易港一流的营商环境和公平竞争市场秩序，增强企业商业秘密保护意识，规范和推动企业商业秘密保护管理工作，提升企业对泄密风险的管控能力和水平，优化公平竞争的营商环境有着重要的技术指导作用。

# 商业秘密保护管理规范

## 1 范围

本文件规定了商业秘密保护的基本要求、人员管理、涉密区域管理、涉密信息管理、检查和改进、维权及服务等内容。

本文件适用于企业商业秘密的保护管理工作，以及科技园区、经济开发区、科研院所、重点实验室、特色小镇、行业协会、第三方社会服务机构的商业秘密保护管理工作。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系要求

GB/T 39786-2021 信息安全技术信息系统密码应用基本要求

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**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、经营信息等商业信息。

注：“不为公众所知悉”、“具有商业价值”和“相应保密措施”的具体内容见《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》等有关法律法规、司法解释的规定。

3.2

**技术信息 technical information**

与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息。

3.3

**经营信息 commercial information**

与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息。

注：客户信息包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

3.4

**涉密载体 secret-related 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介质，包括磁性介质、光介质和纸质材料。

## 4 基本要求

### 4.1 机构和人员

4.1.1 应由企业的法定代表人或授权人统筹管理商业秘密保护工作，应设立专门机构或依托相关部门开展商业秘密保护工作。

4.1.2 应配备保密员，宜在涉及商业秘密保护的重点部门配备专职保密员。

4.1.3 商业秘密保护部门/机构和保密员应履行包括但不限于以下职责：

a) 负责商业秘密保护相关制度的建立、实施、检查及改进；
b) 组织相关部门做好商业秘密的识别、定密及日常登记与管理；
c) 组织相关部门制定适宜的保密措施；
d) 组织企业员工进行商业秘密保护培训；
e) 负责涉嫌侵犯商业秘密行为、涉嫌侵犯商业秘密罪案件的证据的整理、搜集、举证、协助调查取证等维权工作。

4.1.4 派出机构、投资的企业和关联企业可参照设置保密机构和保密员。

### 4.2 保密措施

4.2.1 应制定商业秘密保护管理制度、培训制度和奖惩制度。可根据企业规模和实际业务需求制定包括但不限于下列制度：

a) 涉密文件管理制度；
b) 涉密物品管理制度；
c) 涉密计算机账户、数据管理制度；
d) 涉密场所管理制度；
e) 涉密人员管理制度；
f) 外来人员保密制度；
g) 合作单位保密制度；
h) 客户信息保密制度；
i) 考核评级制度；
j) 网上处理机制。

4.2.2 应分析确定商业秘密保护的重点部门和重点岗位，可划定商业秘密保护重点区域，宜实行物理隔离保护。

4.2.3 应在合同条款中规定商业秘密保护要求，或与合作单位单独签订商业秘密保护合同/协议。

4.2.4 一般性的保密措施应符合下列保密要求：

a) 限制了接触范围；
b) 明确了接触的准许条件或者采取了限制接触的技术手段；
c) 对接触人员明确赋予了未经授权不应使用、披露的义务；

d) 接触到商业秘密的人员都能显然识别和认识到其为商业秘密。

## 5 人员管理

### 5.1 工作人员

#### 5.1.1 入职

5.1.1.1 应对拟入职工作人员进行保密事项提醒，告知其有保护企业商业秘密的义务，并提醒其不应泄露前雇主的商业秘密。

5.1.1.2 新入职涉密岗位人员（含转岗）应签订商业秘密保护合同/协议，根据其岗位保密程度明确约定保密范围和期限，双方的权利和义务以及违约责任等。

5.1.1.3 涉密重点岗位员工入职前宜做背景调查。根据需要，可对相关高级管理人员、高级技术人员开展入职前核查，包括查验犯罪记录。

#### 5.1.2 宣传培训

5.1.2.1 应对新入职员工进行保密培训，以确保其：

a) 理解商业秘密权利、义务，树立保密意识；
b) 理解企业商业秘密管理相关规定；
c) 理解其岗位的保密责任。

5.1.2.2 制定年度计划，采取集中培训、发放资料、网络培训等方式开展年度常态化商业秘密保护宣传及培训。

5.1.2.3 宜对签订商业秘密保护合同/协议的人员进行保密考核，考核结果存档，作为奖惩依据。

#### 5.1.3 日常要求

5.1.3.1 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，包括：

a) 涉密信息及载体应及时上报，由保密员归档统一管理；
b) 使用涉密信息应履行登记手续；
c) 涉密电子文档、数据按规定途径和要求使用、流转；
d) 离开工作岗位前及时下线工作账户，并设置电脑锁屏。

5.1.3.2 未经商业秘密保护机构/部门审批，不应出现下列行为：

a) 登录未授权账户；
b) 超范围使用涉密文件资料、物品、数据；
c) 复制、发送涉密电子文档；
d) 将涉密电子文档存于未授权载体或网络空间；
e) 拍摄、摘抄涉密资料；
f) 拍摄、测绘、仿造涉密物品；
g) 进入非授权涉密区域；
h) 披露企业未公开的信息。

5.1.3.3 中高层管理人员和涉密重要岗位员工不宜出现下列行为：

a) 兼职或入股与所在企业经营相关、相同或相似的企业；
b) 同与所在企业有交易关系、竞争关系、行业相同或相似的国内外企业进行涉密交易；

c） 组建、参与组建或变相投资与所在企业经营相关相同或相似的企业。

#### 5.1.4 离职

5.1.4.1 涉密岗位员工离职前，宜采取适当措施进行脱密。

5.1.4.2 离职员工应主动移交一切涉密载体和物品，包含但不限于：

a） 涉密文件资料、数据及其载体、物品；

b） 账户信息，如账号、密码；

c） 工作电脑；

d） 门禁卡。

5.1.4.3 可开展离职检查，检查内容为：

a） 检查工作电脑数据是否完整；

b） 检查工作账户：近期是否有异常操作，如异常查询、下载、拷贝、修改、删除；邮箱邮件收发记录；

c） 离职前一定期限内的涉密文档、数据的查阅和使用情况。

5.1.4.4 宜进行离职谈话，告知离职员工不应：

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、发送涉密电子文档、数据；

c） 删除、更改账户；

d） 披露、使用商业秘密。

5.1.4.5 高级技术人员、高级管理人员及其他负有保密义务的人员（如职业经理人、技术、采购、销售等涉密重点岗位人员）可签订竞业限制协议等商业秘密保护确认文书，并掌握离职员工在竞业限制期限内的任职情况。

5.1.4.6 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。

### 5.2 来访人员

5.2.1 来访人员进入涉密区域应经审批，履行进出登记，佩戴临时证件。

5.2.2 来访人员进入涉密区域，受访部门应安排人员陪同，限制来访者使用具有录音、摄像、拍照、信息存储等功能的设备。

### 5.3 其他人员及活动

5.3.1 与供应商、客户、合作方签订保密协议，约定保密内容和范围、保密责任和义务及违约责任。

5.3.2 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，并签署保密协议。

5.3.3 涉及商业秘密的会议或其他活动，应采取下列保密措施：

a） 选择具有保密条件的场所；

b） 根据工作需要，限定参加人员的范围，指定参与涉密事项的人员；

c） 告知参加人员保密要求，必要时签订保密承诺书；

d） 通过拍照、摄像等方式做好记录。

## 6 涉密区域管理

6.1 企业应识别涉密区域，门口张贴涉密区域标志。宜将下列部门或地点列为涉密重点区域：

a) 研发设计、信息管理、财务等部门；
b) 控制中心、服务器机房等；
c) 涉密档案、涉密载体存放地点；
d) 未公开的样品存放地点；
e) 模具、专用夹具、重要零部件等的存放区；
f) 重要原材料、重要半成品等保密物资存放区。

6.2 涉密区域应采取封闭式管理，通过安保人员、门禁、身份识别卡、摄像头等措施进行管控，限制具备拍摄、录音、存储等功能的智能设备使用。

6.3 涉密区域限制外来人员访问、参观、考察，确因工作需要进入涉密区域应按 5.2 进行管理。

6.4 涉密重点区域实行进出登记和保密告知，应有如下保护措施：

a) 划定相对独立的空间，进出口有涉密区域标识；
b) 设有门禁隔离设施，涉密区域进入需获得许可；
c) 进出口处设置报警装置，非法闯入能立即告警；
d) 限制使用具有录音、摄像、拍照、信息存储等功能的设备；
e) 必要时采取网络隔离阻断。

6.5 应在涉密区域内设置画报、标语，营造商业秘密保护氛围。

## 7 信息管理

### 7.1 信息处置

#### 7.1.1 定密

7.1.1.1 根据需要保护的技术信息、经营信息，确定商业秘密内容并按重要性实行分级管理，一般分为核心秘密、重要秘密和一般秘密三个等级，定密结果应由法定代表人或其授权人审批。

7.1.1.2 下列可认定为公众所知悉的信息不应作为企业保护的商业秘密：

a) 在所属领域属于一般常识或者行业惯例的；
b) 仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；
c) 已经在公开出版物或者其他媒体上公开披露的；
d) 已通过公开的报告会、展览等方式公开的；
e) 所属领域的相关人员从其他公开渠道可以获得该信息的；
f) 公知信息和基础理论；
g) 已申请并公开的专利；
h) 企业以其他方式公开的信息；
i) 可通过合法渠道获得的信息；
j) 法律法规规定的其他情形。

#### 7.1.2 解密

7.1.2.1 企业认为不需要继续保密的信息可予以解密，可采取的解密方式为：

a) 移出涉密区域；

b） 消除或涂改密级标识、提示；
c） 电子文档解密；
d） 发文公布。

7.1.2.2 信息解密前，根据需要对即将解密的信息采取相应手段（申请专利、版权等）做好知识产权保护工作。

#### 7.1.3 隐密

7.1.3.1 下列情形涉及商业秘密信息时，应予隐密：
a） 尽职调查时；
b） 与供应商、客户、合作方等的沟通和信息往来中；
c） 信息公开、发布、流转时。

7.1.3.2 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。

#### 7.1.4 销毁

7.1.4.1 销毁涉及商业秘密的文件、资料、电子信息、载体和物品，应由保密员列出销毁清单，经商业秘密保护机构/部门审批后实施。

7.1.4.2 采取下列方式对销毁过程进行监督管理：
——在视频监控范围内销毁；
——不少于 2 名员工见证下销毁；
——对销毁过程录像。

7.1.4.3 应采取合适的方式妥善销毁：
——文件、资料应粉碎成颗粒状或焚烧处置；
——电子信息应利用彻底删除软件永久删除；
——其他合适的方式。

### 7.2 常规管理

#### 7.2.1 涉密文件、资料管理

7.2.1.1 应有密级、保护期限等标识，归档存放。

7.2.1.2 由部门专兼职保密员登记造册，按权限使用，查阅、借阅、续借应履行登记手续。

7.2.1.3 复制（复印、打印、扫描、摘抄等）、跨区域转移、向第三方披露或提供第三人使用前应履行审批和登记手续。

7.2.1.4 新闻发布、论文发表、专利申请等信息发布和公开时，应由商业秘密保护部门/机构对信息进行审核。

7.2.1.5 销毁正式发布的文件（含复制文件）应经商业秘密保护机构/部门、法定代表人或其授权人审批，参照 7.1.4 执行。

#### 7.2.2 涉密账户、电子信息管理

##### 7.2.2.1 权限管理

7.2.2.1.1 应对设备、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按“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；
c) 合理设定不同账户的访问、操作、查看等权限及其使用期限；
d) 合理设定不同账户的互联网使用权限。

7.2.2.1.2 权限到期、人员转岗、项目或事项变更时应重新授权。

7.2.2.1.3 人员离职时应回收相应权限。

#### 7.2.2.2 密码管理

7.2.2.2.1 各类设备、数据库和应用系统应设有账户和密码，不应使用默认密码，不可保存密码自动登录。

7.2.2.2.2 根据企业的业务类型，采取适当的账户、密码管理方式，如：

a) 限制使用简单密码，应使用数字、字母、符号等组合密码；
b) 应不定期更改密码，间隔宜不长于 3 个月；
c) 输错密码一定次数锁定账户。

### 7.2.3 涉密载体、物品管理

7.2.3.1 涉密信息存放的硬盘、光盘、磁性介质、U 盘等各类存储设备，应妥善保存、归档登记。

7.2.3.2 涉密载体、物品的存放地点宜设为涉密重点区域，宜采取物理隔离的方式进行保护。

7.2.3.3 未经商业秘密保护部门/机构、法定代表人或其授权人审批，不得拍摄、测绘或仿造。

7.2.3.4 由部门专兼职保密员登记造册，按权限使用，领用应履行登记手续。

7.2.3.5 跨区域转移应履行审批手续，必要时采取防护措施。

7.2.3.6 报废销毁应经商业秘密保护部门/机构、法定代表人或其授权人审批，采取合适的方式妥善处置，参照 7.1.4 执行。

## 7.3 数字化信息安全

### 7.3.1 数字化信息管理

7.3.1.1 涉密数字化数据应存储于企业授权的存储设备和应用系统，不应存储于非授权存储设备、网络空间。核心秘密和重要秘密数据应采用加密方式存储。

7.3.1.2 指定专人进行解密操作，员工按照权限使用加密数据。

7.3.1.3 员工超出权限需要查阅或使用加密数据的，应经商业秘密保护机构/部门批准，在查阅或使用完成后，予以删除，不应擅自使用。

7.3.1.4 宜在各类场景进行保密义务提醒，如：

a) 在账户登录提示、账户登录后的主界面设置保密义务提醒；
b) 在涉密电子文档首页、页眉、页脚、页面水印等设置保密义务提醒；
c) 在涉密音视频开头提示保密义务。

7.3.1.5 应定期对涉密数据进行备份，妥善保存备份数据。

### 7.3.2 数字化信息流转

7.3.2.1 收发涉密数据应使用唯一出入口，不应流转至不相关的人员或系统。

7.3.2.2　内部局域网应与互联网隔离，涉密数据网上传递应通过内部局域网或加密的互联网通道完成。
7.3.2.3　通过邮件发送涉密数据时，应设置加密和签名，可限定文档打开次数、打开时限和编辑权限等。
7.3.2.4　对外发送涉密数据应采取加密措施，数据发送与密钥发送不宜采用同一通道。
7.3.2.5　应对涉密数据拷贝采取限制措施，经审核批准后方可拷贝，妥善保存拷贝记录。
7.3.2.6　应与客户、合作单位等涉密数据接收单位签订保密协议。

#### 7.3.3　安全防范

7.3.3.1　应充分考虑设备、系统的安全性，做好账户、密码的收集、存放和传输的安全工作。宜参照GB/T 22080-2016的要求开展企业信息安全管理工作。
7.3.3.2　企业信息系统的密码管理宜参照GB/T 39786执行。
7.3.3.3　做好病毒防范和病毒库的升级、查杀病毒等工作。
7.3.3.4　定期进行安全检查，发现系统漏洞及时修补。
7.3.3.5　用户的操作行为应有日志记录，可实时报告异常入侵、登录、获取信息的行为。

### 7.4　对外合作

#### 7.4.1　商务活动

采购、销售、委托开发、委托生产、参展等商务活动时应注意：

a)　开始商务谈判前或提供涉密信息前，应与对方签署保密协议；
b)　参展过程中通过遮挡、与展览方签订保密协议等方式降低泄密风险；
c)　对协议履行过程中涉密信息的使用情况和泄密情况进行监督管理，保留证据。

#### 7.4.2　技术合作

技术合作中应调查合作方的商业秘密管理能力，优先选择商业秘密管理能力强的合作方。

## 8　检查和改进

8.1　应开展商业秘密保护管理情况检查，检查内容包括但不限于：

a)　商业秘密保护制度建立情况；
b)　涉密人员管理情况；
c)　涉密区域管理情况；
d)　商业秘密的定密、解密、脱密、隐秘情况；
e)　涉密文件、资料的管理情况；
f)　涉密账户、电子信息的管理情况；
g)　涉密载体、物品的管理情况。

8.2　在检查过程中，发现有泄密情况及隐患的，应及时采取纠正、预防措施。

## 9　维权

### 9.1　应急处置

9.1.1 应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。
9.1.2 培训和引导员工对商业秘密可能泄露的异常状态保持警觉，发现可能泄密迹象及时报告上级。
9.1.3 出现商业秘密泄露的征兆或者迹象时，企业应：
a) 迅速进行处置，防止信息扩散；
b) 采取措施，将危害和损失控制在最小限度内；
c) 启动对商业秘密泄露的核查、确认和评估，查明原因、责任人。

### 9.2 证据收集

企业发现商业秘密被侵犯的迹象、线索时，应及时与管辖地的商业秘密保护服务机构、市场监督管理部门等联系，在其指导下搜集下列证据，必要时进行证据保全公证：
a) 泄密信息的具体内容、载体，企业已采取的保护措施；
b) 泄密信息为一般公众不知悉或者无法轻易获得的信息；
c) 可能的泄密途径；
d) 可能与泄密信息有关的人员（如在职员工、离职员工、退休员工）的信息：在本企业的工作经历、工作内容、接触到的涉密信息，在本企业接受保密培训的记录，与企业签订的商业秘密保护合同、协议。
e) 可能与泄密信息有关的第三方等；
f) 侵犯涉密信息的具体行为表现；
g) 对方使用泄密信息发生侵权可能导致的后果。

### 9.3 维权途径

9.3.1 根据证据收集情况，企业可依法采取下列方式进行维权：
a) 向市场监督管理部门投诉举报；
b) 向公安机关报案；
c) 向人民法院提起民事诉讼；
d) 申请商事仲裁。
9.3.2 涉及国家秘密的应向国家安全部门报告。

## 10 科技园区管理

### 10.1 平台建设

优势产业集聚的园区、经济开发区、特色小镇、行业协会等，可根据自身力量和企业需求，设立涵盖商业秘密保护的服务平台，为辖区企业规范商业秘密保护提供服务。

### 10.2 工作机构

10.2.1 应合理设置岗位，配置商业秘密保护专（兼）职工作人员，建立工作人员管理制度，明确工作职责，并签订保密协议，保障服务平台正常运营。
10.2.2 宜吸引商业秘密保护专家团队、调解机构、律师事务所等第三方社会组织和人员，聚集、整合服务资源。
10.2.3 可协调下列商业秘密保护相关部门在园区设立服务指导站：
a) 市场监督管理部门；

b） 公安机关、检察院、法院；
c） 仲裁机构。

10.2.4 宜设独立的商业秘密保护服务窗口，也可依托园区知识产权保护服务窗口提供服务。

## 10.3 工作要求

### 10.3.1 宣传培训

10.3.1.1 应开展辖区商业秘密保护宣传，可采取的方式为：
a） 定期举办商业秘密保护培训班；
b） 编制、印发商业秘密保护宣传资料；
c） 利用园区媒体平台宣传等。

10.3.1.2 可组织适合企业不同层次人员的商业秘密保护专题培训：
a） 对企业法定代表人、股东、高级管理人员开展商业秘密保护重要性和必要性培训；
b） 对企业从事商业秘密保护工作的专兼职人员开展商业秘密保护实务及案例培训；
c） 对企业商业秘密保护重点岗位人员开展商业秘密保护意识培训；
d） 对企业员工开展商业秘密保护知识普及培训；
e） 利用行业协会、学会、商会等渠道将维权成功的案例向企业广泛宣传。

### 10.3.2 商业秘密保护指导

10.3.2.1 通过走访调研，了解企业商业秘密保护需求，有针对性地开展商业秘密保护指导工作。

10.3.2.2 接待和解答企业商业秘密保护咨询，提供商业秘密保护相关资料查询服务。

10.3.2.3 引导园区企业建立和完善商业秘密保护工作体系，包括但不限于：
a） 界定商业秘密保护范围；
b） 建立和完善商业秘密保密制度；
c） 建立和完善商业秘密分类管理制度；
d） 建立和完善商业秘密使用管理制度；
e） 建立和完善商业秘密保护的应急反应机制。

10.3.2.4 引入第三方社会服务机构，开展商业秘密保护服务，包括但不限于：
a） 商业秘密培训；
b） 提供商业秘密专业知识咨询；
c） 协助企业建立商业秘密保护机制；
d） 开发和维护涉密文件、数据的信息管理系统；
e） 协助被侵权企业收集证据和协助维权。

### 10.3.3 维权协助

10.3.3.1 当企业商业秘密涉嫌被侵权，向园区平台申请协助时，应协助企业搜集、整理维权材料。

10.3.3.2 根据被侵权企业提供的材料，引导企业采取合理的依法维权途径。

10.3.3.3 依据被侵权企业的意愿，协助执法部门开展泄密核查、现场检查及案件查处等，并协助做好调解服务。

10.3.3.4 配合市场监督管理部门、仲裁机构、法院等部门化解争议。

# 参 考 文 献

[1] 《中华人民共和国反不正当竞争法》
[2] 《中华人民共和国保守国家秘密法》
[3] 《中华人民共和国保守国家秘密法实施条例》
[4] 国家市场监管总局《商业秘密保护规定》（征求意见稿）(2020年)
[5] 《国家工商行政管理局关于禁止侵犯商业秘密行为的若干规定》
[6] 《海南自由贸易港知识产权保护条例》
[7] DB33/T 2273-2020 商业秘密保护管理与服务规范（浙江省地方标准）
[8] 中国专利保护协会《企业商业秘密管理规范》（征求意见稿2021年）