ICS 03.100.01
CCS A 10

DB4420

中　　山　　市　　地　　方　　标　　准

DB4420/T 54—2024

# 企业商业秘密保护管理规范

2024-06-26 发布　　2024-08-26 实施

中山市市场监督管理局　　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　总则 ..... 1
5　制度建设与管理 ..... 2
6　人员管理 ..... 5
7　信息系统管理 ..... 6
8　物理空间管理 ..... 8
9　泄密应急处置措施 ..... 8
10　维权指引 ..... 8
附录A（资料性）　商业秘密保密协议 ..... 11
附录B（资料性）　竞业限制协议 ..... 19
附录C（资料性）　商务合作保密协议 ..... 24
附录D（资料性）　构成商业秘密的证据材料 ..... 29
参考文献 ..... 30

# 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。

本文件由中山市市场监督管理局（知识产权局）提出并归口。

本文件起草单位：中山市深中标准质量研究中心、广州中新知识产权服务有限公司、中山市家电知识产权快速维权服务中心、中山市知识产权保护中心。

本文件主要起草人：叶俊文、郝爱昕、陈程、陈淑曲、孙倩、欧慧敏、郭金丰、江承成、贺丽君、黄嘉慧、黄石娟、杜展浩、殷欢、刘皇增、曹璐、吴佩珊。

# 企业商业秘密保护管理规范

## 1 范围

本文件规定了企业商业秘密保护的术语和定义、总则、制度建设与管理、人员管理、信息系统管理、物理空间管理、泄密应急处置措施、维权指引。

本文件适用于企业商业秘密保护管理。若涉及国家秘密应按照《中华人民共和国保守国家秘密法》及相关规定要求执行。

## 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 信息技术 安全技术 信息安全管理体系 要求

GB/T 29490 企业知识产权合规管理体系 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。

3.2

**涉密载体 secret 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纸介质、磁介质、光盘等各类载体。磁介质载体包括计算机硬盘、软盘和录音带、录像带等。

3.3

**涉密人员 secret-related personnel**

根据工作职责或者保密协议有权接触、使用、掌握商业秘密的企业员工或其他人。

## 4 总则

### 4.1 一般要求

4.1.1 应明确界定商业秘密的内容和范围，明确涉密信息的密级，对含有保密信息的载体采取相应保密措施。

4.1.2 应全面分析企业经营管理各个环节，逐一梳理企业的技术信息、经营信息等商业信息，对照“不为公众所知悉”、“具有商业价值”和“保密措施”界定企业商业秘密范围。

### 4.2 保密范围

4.2.1 对于技术信息，应明确载体中哪些数据、指标、尺寸或技术方案等构成商业秘密。
4.2.2 对于技术信息，可选择专利权或商业秘密进行保护。
4.2.3 在以下情形之一时，宜以专利权进行保护：

a) 技术信息在商业产品/服务中易为公众所接触；
b) 客户不愿签署保密协议；
c) 有可能对外进行许可；
d) 相关技术人员流动性高；
e) 法律法规或政府机关要求公开技术信息；
f) 属于可能或者将会对技术标准产生重大贡献的技术方案，很有可能形成标准必要专利；
g) 可以预见或已经存在与外部的合作关系；
h) 可通过反向工程、自行研发获得相同的技术；
i) 技术方案处于更新换代较快的领域。

4.2.4 在以下情形之一时，宜以商业秘密进行保护：

a) 属于企业的内部信息；
b) 在企业内部只有少数员工知晓；
c) 接触该信息的人员都愿意签署保密协议或承诺书；
d) 技术方案本身先进性程度较高，在一定时期内难以被他人研发出来，也不可能从其他渠道获取同样的技术；
e) 无法通过专利权或者著作权保护；
f) 技术方案难以进行专利侵权技术比对的。

### 4.3 管理原则

4.3.1 宜建立完善的商业秘密保护管理体系，可参照 GB/T 29490 相关要求执行。
4.3.2 宜建立保密管理机构或领导小组，如设立企业保密委员会，规模较小的企业可由企业相关管理部门归口管理，设置保密专员。
4.3.3 应定期对员工开展保密教育，增强员工保密观念和自觉性，提高员工保密的一般常识和技能。
4.3.4 应对商业秘密日常保密情况进行检查和监督，及时发现和处理泄密隐患及问题。
4.3.5 应制定保密工作激励机制，宜奖励在商业秘密保护中作出突出成绩和贡献的部门和人员。
4.3.6 应维护保密规章制度的权威性，追究违反保密制度、泄露商业秘密人员的责任。
4.3.7 商业秘密被侵犯时，应及时采取补救措施，搜集相关证据，提出维权方案，寻求行政或司法保护。

## 5 制度建设与管理

### 5.1 制度与协议

#### 5.1.1 制度建设

5.1.1.1 应制定总体的保密制度及相应的惩罚措施，对企业保密信息的定义、保密信息的分级、员工保密义务、违反保密义务的罚则等进行规定。
5.1.1.2 应对涉密文件管理、涉密人员管理、涉密区域管理、涉密载体管理、计算机网络及信息系统管理、人员流动及保密应急处置预案等制定企业保密制度。
5.1.1.3 保密制度与企业其它制度应相互协调，形成有效的监督与约束机制。

5.1.1.4 应定期开展商业秘密保护制度的有效性评估，跟踪、判别企业发展过程中的涉密风险，及时更新、完善保密制度和保密措施。

#### 5.1.2 协议

5.1.2.1 应与员工签订保密协议或者在劳动合同中明确约定保密义务，保密协议可参考附录 A。

5.1.2.2 宜与知悉或接触商业秘密的高级管理人员、高级技术人员或其他负有保密义务的员工签订竞业限制协议，竞业限制协议可参考附录 B。及时评估员工是否需要履行竞业限制义务，并作相应的调整。

5.1.2.3 涉及商业秘密的磋商谈判开始前，应先签订商务合作保密协议或保密承诺，商务合作保密协议可参考附录 C。

### 5.2 商业秘密信息管理

#### 5.2.1 一般要求

5.2.1.1 商业秘密信息的产生、保存、流转、复制、发布、解密、销毁等均应保留记录。应根据商业秘密信息的重要性及储存成本规定记录留存时间。

5.2.1.2 认定技术信息和经营信息是否为商业秘密，可从保密必要性、保密可能性、保密效果等方面评估。

5.2.1.3 应根据商业秘密信息自身的生命周期长短、技术成熟程度、信息现实或潜在价值大小和市场需要程度等因素，确定其密级和保密期限。

#### 5.2.2 秘密点确定

5.2.2.1 技术信息主要包括与技术有关的结构、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。

5.2.2.2 经营信息主要包括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。

5.2.2.3 技术信息的秘密点确定，应考虑以下内容：

a) 明确商业秘密信息的具体内容；
b) 技术秘密“三性”检验。应综合考虑秘密性、价值性、保密性三个方面，做三性评价；
c) 合理确定秘密点的数量。宜从创造性、贡献度、成本等维度来确定秘密点数量。

5.2.2.4 经营信息的秘密点确定，应从主观布局和经营管理信息累积及信息的更迭做综合评估。

5.2.2.5 技术秘密点应根据技术进步和维权的需要及时调整。

#### 5.2.3 分级管理

5.2.3.1 商业秘密可分为核心商业秘密（绝密级）、重要商业秘密（机密级）及普通商业秘密（秘密级），宜实行分级管理。商业秘密信息的级别应在其载体上明确标识。

5.2.3.2 核心商业秘密确定依据包括但不限于：

a) 保密价值高；
b) 内部扩散或向外部泄露威胁到企业生存、发展，削弱企业核心竞争力的；
c) 泄露对企业经济利益造成特别严重损失、危害的；
d) 泄露对业务开展造成严重影响的。

5.2.3.3 重要商业秘密确定依据包括但不限于：

a) 保密价值中等；
b) 内部扩散或向外部泄露可能威胁到企业生产、发展，削弱企业市场竞争力的；

c） 泄露对企业经济利益造成严重损失、危害的；
d） 泄露对业务开展造成重要影响的。

5.2.3.4 普通商业秘密确定依据包括但不限于：
a） 保密价值相对较低；
b） 泄露对业务造成轻微影响的。

5.2.3.5 核心商业秘密宜仅限于为核心管理层或特定部门部分人员知晓；重要商业秘密宜仅限于在特定部门或项目组内部知晓；普通商业秘密仅允许在企业一定范围内部流通。

5.2.3.6 应建立商业秘密分级管理信息清单，内容包括商业秘密信息名称、密级、管理人、载体、查阅范围等。

### 5.2.4 解密

5.2.4.1 企业认为不需要继续保密的信息可予以解密，可采取的解密方式包括但不限于：
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。

5.2.4.2 信息解密前，根据需要对即将解密的信息可采取相应措施，做好保护工作（如专利申请、版权登记等）。

### 5.2.5 销毁

5.2.5.1 删除商业秘密信息或销毁含有商业秘密的载体，应经批准后实施。

5.2.5.2 应采取合适的方式妥善销毁，包括但不限于：
a） 纸质类资料作粉碎性处理；
b） 电子信息类的存储硬盘、光盘、U 盘等介质与信息系统内的记录进行删除；
c） 含有核心秘密的电子信息载体宜作销毁处理。

5.2.5.3 可采取视频监控、录像、见证等方式对销毁过程进行监督管理。

## 5.3 商业秘密载体管理

### 5.3.1 纸质文件

5.3.1.1 应有密级、保护期限等标识，实行登记管理、归档存放。

5.3.1.2 按权限使用，查阅、借阅等应履行登记手续。

5.3.1.3 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，复制件与原件的密级、保密期限相同。

### 5.3.2 电子信息载体

5.3.2.1 涉密数据应存储于企业授权的存储设备和应用系统，应采用加密方式存储。

5.3.2.2 涉密电子信息物理载体的采购、维护应进行归档登记，并选用安全稳定、运转正常的电脑、手机、硬盘等存储介质。存储介质送外维修前应经审批，并使用专业工具擦除介质中的数据。

5.3.2.3 对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施。

5.3.2.4 涉密电子信息存储系统应定期进行安全检查，发现系统漏洞及时修补。

### 5.3.3 产品

5.3.3.1 涉密项目的半成品、样品应由专人管理，放置在保密柜或专门的存储室保管。

5.3.3.2　涉密项目的不良品应交由专人处理或报废，不应随意丢弃。

## 5.4　内部保密管理

### 5.4.1　研发流程管理

应完整保留研发过程中的实验记录（包括失败的研发记录）。宜采用研发管理系统进行项目管理，研发资料应定期上报并核查，研发文件应有研发人员签名和签署日期。

### 5.4.2　生产流程管理

对特有的制作工艺流程、涉及生产设备的改进技术应进行保密管理。涉密的厂房、车间等生产经营场所应限制来访或进行区分管理。

### 5.4.3　日常保密管理

5.4.3.1　通过保密协议、章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的人员（员工、前员工、供应商、客户、来访者等）提出保密要求。

5.4.3.2　办公使用后废弃的图纸、文件、磁盘、打字机色带等宜彻底粉碎销毁。

5.4.3.3　涉密区域需要外部人员进行维修、保洁、安装等作业，或涉密载体、计算机设备等需要携带外出进行修理、维护时，应当采取合理保密措施，并指定专人进行现场监督。

5.4.3.4　对外宣传交流应由宣传部门承担保密初审工作，建立对外宣传审查制度。

5.4.3.5　应建立论文或科技成果发表、项目申报审查制度，对文件材料预先审查，不应涉及专有技术秘密、在研产品、精确技术参数和保密数据等。

5.4.3.6　专利申请时，应先确定需要按照商业秘密进行保护的技术内容和范围。确定为按照商业秘密进行保护的技术内容，不应写入专利申请文件，不应在专利授权审查、专利无效宣告程序中泄露。

5.4.3.7　应建立信息对外披露的保密审查责任制，明确信息对外发布的保密审查程序和主管领导机构及工作人员；在提供商业秘密前，应与信息接收方签署保密协议。

## 5.5　外部商务合作保密管理

5.5.1　与第三方进行合作时，企业应做好与第三方的保密管理。重点包括但不限于以下情形：

a)　合作研发、委托研发；
b)　委托加工及定制、受托生产；
c)　合作供应、经销；
d)　临床试验、检测检验；
e)　运输、仓储；
f)　产品注册、法律事务、会计、审计等。

5.5.2　应与可能获取、接触本企业保密信息的第三方签订保密协议，明确相关方的保密义务及违约责任。

5.5.3　应在合同中明确技术成果商业秘密归属，对共有商业秘密，应要求其他权利人履行保密义务。

5.5.4　向第三方或政府审评审批机构等主体提供涉密资料时，应当对相关涉密资料进行明确的涉密标识，并要求相关方采取合理的保密措施。

# 6　人员管理

## 6.1　岗位划分

6.1.1 日常工作中产生、经管或者经常接触、知悉核心商业秘密的岗位划分为核心商业秘密岗位。
6.1.2 日常工作中产生、经管或者经常接触、知悉重要商业秘密的岗位划分为重要商业秘密岗位。
6.1.3 日常工作中偶尔需要接触企业普通商业秘密的岗位划分为普通商业秘密岗位。

### 6.2 涉密人员分类

6.2.1 以所在岗位接触到的商业秘密等级为原则，将涉密人员分为核心商业秘密人员、重要商业秘密人员及普通商业秘密人员。涉密人员包括但不限于以下人员：

a) 企业董事、经理、合伙人等高级管理人员；
b) 从事生产、研发、策划、财务等重要岗位的人员；
c) 从事法务、办公室等登记和管理商业秘密的人员；
d) 其他可能接触到商业秘密的人员。

6.2.2 应与核心商业秘密人员、重要商业秘密人员及普通商业秘密人员签订保密协议，并与核心商业秘密人员及重要商业秘密人员签订竞业限制协议。
6.2.3 应对涉密人员明确其保密范围和接触的商业秘密信息。

### 6.3 入职

6.3.1 人力资源管理部门应了解员工是否与原单位签订竞业限制协议、竞业限制期限是否已经届满、竞业限制协议是否提前解除等情况，并要求员工签订不侵犯他人商业秘密保证书。
6.3.2 新入职的涉密人员应与其签订保密协议，必要时签订竞业限制协议。
6.3.3 应通过面谈或培训等方式明确告知保密义务等注意事项。

### 6.4 转岗

6.4.1 员工转岗到涉密岗位的应签订与其工作内容相适应的保密协议。
6.4.2 员工调离涉密岗位的应明确是否已签署与其工作内容相适应的的保密协议，并督促转岗员工做好保密材料交接工作，及时做好涉密权限调整，做好脱密管理工作。

### 6.5 离职或退休

6.5.1 人力资源管理部门应与相关部门对离职或退休员工进行保密谈话，明确提出保密要求，并在谈话笔录上进行签字确认。
6.5.2 应要求离职员工登记、返还、清除、销毁其接触或获取的商业秘密及其载体，继续履行保密义务。
6.5.3 应结合员工离职前的岗位、工作内容进行综合评估，确定该员工是否需要履行竞业限制义务，并在办理离职手续时明确告知。
6.5.4 应设置离职或退休交接清单，由员工所在部门、人力资源、行政、财务等相关部门进行保密资料、载体等的清退，并在交接清单上设置保密要求条款，由员工本人签字确认。

## 7 信息系统管理

### 7.1 信息安全管理体系

企业宜按照 GB/T 22080 的要求建立信息安全管理体系，以最大化降低信息安全风险。

### 7.2 信息安全管理

#### 7.2.1 权限

7.2.1.1 信息系统的管理员权限应在不同人员之间进行分配，避免由超级管理员管理整个系统或若干个系统的情况。

7.2.1.2 信息系统的权限管理应保留记录日志，用于定期检查各信息系统用户的访问权限、特别授权等权限管理是否存在漏洞。

### 7.2.2 访问控制

7.2.2.1 访问控制应按照以下两个原则：

a) “按需所知”原则：只允许访问执行任务所需的信息；

b) “按需使用”原则：只允许访问执行任务所需要的信息处理设施（如 IT 设备、应用程序、规程、场所等）。

7.2.2.2 宜通过用户注册和注销分配访问权。对用户 ID 的管理包括但不限于以下内容：

a) 宜使用唯一用户 ID，使得用户与其行为链接起来，并对其行为负责。必要时，经过批准且形成文件情形下，允许使用共享 ID；

b) 应定期识别并删除或禁用冗余的用户 ID，确保冗余的用户 ID 不会发给其他用户。

7.2.2.3 宜限制对信息和应用系统功能的访问，可采取措施包括但不限于：

a) 提供控制访问应用系统功能的选择菜单；

b) 控制用户的访问权，如读、写、删除和执行；

c) 限制输出中包含的信息。

7.2.2.4 宜通过安全登录控制对系统和应用的访问。可选择适当的身份鉴别技术，如密码手段、智能卡、令牌或生物特征识别方法。

7.2.2.5 若采用密码手段鉴别系统用户的身份信息，应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等。

7.2.2.6 应具有登陆失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出。

7.2.2.7 所有员工和外部用户对信息和信息处理设施的访问权在任用、合同或协议终止时，应予以移除，或在变更时予以调整。

### 7.2.3 恶意软件防范

7.2.3.1 宜建立并实现控制用户安装软件的规程。

7.2.3.2 宜确定允许安装的软件类型和不得安装的软件类型（如仅为个人使用的软件，未知的或可疑的潜在的恶意软件）。

7.2.3.3 应安装及定期更新恶意软件检测和修复软件，扫描计算机和介质。执行的扫描宜包括：

a) 在使用通过网络或任何形式的存储介质得到的文件前，需扫描恶意软件；

b) 在使用电子邮件附件和下载前，需扫描恶意软件；

c) 扫描网页的恶意软件。

### 7.2.4 备份

7.2.4.1 应对信息、软件和系统镜像进行备份，并定期测试。

7.2.4.2 应根据业务要求、涉及信息的安全要求、信息重要性等确定备份的程度（如完全备份或差异备份）和频率。

7.2.4.3 备份宜存储在一个远程地点，有足够距离，以避免主办公场所灾难时受到损坏。

7.2.4.4 备份信息保护等级应与原件一致。

### 7.2.5 日志和监视

7.2.5.1 应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。
7.2.5.2 记录日志的设施和日志信息应加以保护，以防止篡改和未授权访问。
7.2.5.3 系统管理员和系统操作员活动应记入日志，并对日志进行保护和定期评审。
7.2.5.4 日志保存时间宜不少于 6 个月。
7.2.5.5 应正确设置计算机时钟以确保审计记录的准确性。可使用链接到源于国家原子钟的无线电广播时间，作为日志生成系统的主时钟，可使用网络时间协议来保持所有服务器与主时钟完全同步。

## 8 物理空间管理

8.1 涉密重点区域包括但不限于：
a) 研发设计、信息管理、财务、人力资源部门核心区域；
b) 实验室、重要生产工作场所；
c) 控制中心、服务器机房等；
d) 涉密档案、涉密载体存放地点；
e) 未公开的样品存放地点；
f) 重要原材料、重要半成品等涉密物资存放区等。
8.2 对涉密重点区域应限制非相关人员进入，确因工作需要进入的应履行审批手续并全程监督。
8.3 应对涉密重点区域明确标示，设置警示标语，醒目提示非被授权人员不得进入无权进入区域。
8.4 涉密重点区域的出入口宜采取以下安保措施：
a) 使用指纹、人脸识别、瞳孔等生物识别技术手段的防尾随门禁，不宜使用刷卡或密码门禁；
b) 配备检测设备以限制携带手机等带有通讯功能的电子设备出入；
c) 配备视频监控及报警系统，对非法闯入或携带违禁品进入实时报警；
d) 设置监控中心并配备专职人员实时监控。
8.5 来访人员进入涉密区域，受访部门可设定参观路线，安排人员陪同，限制来访人员使用具有录音、摄像、拍照、信息存储等功能的设备。

## 9 泄密应急处置措施

9.1 发生商业秘密泄露后，应立即启动应急措施，尽快调查泄密源头或泄密环节及泄密事件相关人员情况，了解泄密的途径和范围。
9.2 根据调查情况形成事件报告，评估危害，由保密机构或相关管理部门成立危机处置领导小组，出具处置方案。
9.3 向泄密人员和企业发警告函，告知泄露商业秘密的法律后果，要求返还相关商业秘密及其载体，并不得再公开和使用，防止泄密范围进一步扩大。
9.4 应及时采取措施固定相关证据，便于后续调查处理。

## 10 维权指引

### 10.1 维权方式

根据初步收集的证据，对商业秘密泄露事件做初步侵权判断，并选择合适的维权方式，包括行政维权、民事维权、刑事控告维权等。

### 10.2 证据收集

#### 10.2.1 认定构成商业秘密的证据材料

证明涉案信息属于商业秘密的证据，应从保密性、价值性、秘密性三个方面进行证据收集，可参见附录D。

#### 10.2.2 证明侵权信息与商业秘密具有同一性的证据

证明商业秘密和涉嫌侵权信息构成实质性相同的证据，可考虑因素包括但不限于：

a) 侵权信息与商业秘密的异同程度；
b) 所属领域的相关人员在商业秘密侵权行为发生时是否容易想到被侵权信息与商业秘密的区别；
c) 侵权信息与商业秘密的用途、使用方式、目的、效果等是否具有实质性差异；
d) 公有领域中与商业秘密相关信息的情况。

#### 10.2.3 证明侵权行为证据材料

10.2.3.1 证明侵权人负有保密义务的证据包括但不限于：

a) 根据法律规定或者合同约定所承担的保密义务；
b) 未在合同中约定保密义务，但根据诚信原则以及合同的性质、目的、缔约过程、交易习惯等，侵权人知道或者应当知道其获取的信息属于权利人的商业秘密。

10.2.3.2 证明侵权人接触商业秘密的证据包括但不限于：

a) 职务、职责、权限；
b) 承担的本职工作或者单位分配的任务；
c) 参与和商业秘密有关的生产经营活动的具体情形；
d) 是否保管、使用、存储、复制、控制或者以其他方式接触、获取商业秘密及其载体。

10.2.3.3 证明侵权人以不正当方式获取、披露或使用商业秘密的行为的证据包括但不限于：

a) 以违反法律规定或者公认的商业道德的方式获取企业的商业秘密；
b) 在生产经营活动中直接使用商业秘密；
c) 对商业秘密进行修改、改进后使用；
d) 根据商业秘密调整、优化、改进有关生产经营活动。

#### 10.2.4 证明侵权损失及合理支出的证据材料

10.2.4.1 可根据研究开发的成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素确定。

10.2.4.2 为调查或制止侵权行为而支出的费用，一般包括律师费、公证费、证据调查费、技术鉴定费等与制止侵权或诉讼支付的直接相关的合理维权支出。

### 10.3 侵权行为

#### 10.3.1 以不正当的手段获取商业秘密

10.3.1.1 以盗窃、贿赂、欺诈、胁迫、电子侵入或其他不正当手段获取权利人的商业秘密，包括但不限于以下情形：

a) 通过秘密窃取商业秘密载体或者未经授权通过摄影、摄像、复制、监听等手段获取商业秘密；
b) 偷阅商业秘密后，凭借记忆将其再现出来；
c) 通过给予财物、高薪、股份或者许诺职位升迁等方式获取商业秘密；
d) 采用虚构事实、隐瞒真相的方式，使他人陷于错误认识而交付商业秘密；
e) 通过对生命、健康、隐私、财产、声誉等方面的损害、威胁或要挟的方式获取商业秘密；

f） 采用黑客、木马等技术手段，破坏他人技术防范措施，侵入计算机信息系统等获取商业秘密；
g） 采取未经授权或者超越授权使用计算机信息系统等方式窃取商业秘密。

#### 10.3.2 合法获取、违约泄露或使用

10.3.2.1 违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。
10.3.2.2 教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

#### 10.3.3 明知或应知

第三人明知或应知商业秘密权利人的员工、前员工或者其他单位、个人实施前述侵犯商业秘密行为，仍然获取、披露、使用或允许他人使用，视为侵犯权利人的商业秘密。

### 10.4 救济途径

#### 10.4.1 行政救济

收集初步证据后可向行政管理部门投诉举报，由商业秘密权利人提出书面申请。

#### 10.4.2 民事救济

商业秘密侵权纠纷可向具有管辖权的人民法院提起诉讼。

#### 10.4.3 刑事救济

符合刑事案件立案标准的商业秘密侵权纠纷可向公安机关提出刑事控告。

#### 10.4.4 其他

其他维权方式可考虑采用调解、仲裁等各类权利救济途径。

# 附 录 A
（资料性）
商业秘密保密协议

商业秘密保密协议见图A.1。

商业秘密保密协议

**甲　　方（用人单位、披露方）：**_____

法定代表人：_____　统一社会信用代码：_____

电　　话：_____　传　　真：_____

地　　址：_____

**乙　　方（劳动者、接受方）：**_____

居民身份证号码：_____

电　　话：_____　职　　务：_____

住　　址：_____

甲、乙双方根据《中华人民共和国反不正当竞争法》、《中华人民共和国劳动合同法》及国家、地方有关规定，双方本着平等自愿、协商一致、诚实守信的原则，为保护甲方商业秘密，于_____年___月日（以下简称“生效日”）在中华人民共和国_____（具体签署地址）签署本保密协议以共同执行：

**第一条**　合同目的描述

乙方了解甲方就其产品、研发、制造、营销、管理、客户、计算机（程序）、营运模式等业务及相关技术、服务投入庞大资金及人物力，享有经济效益及商誉；乙方知悉参与并接触第三条（保密信息范

**图A.1　商业秘密保密协议**

围的条款）所述各项业务机密资料系基于甲方对乙方履行本协议之信赖。乙方若未履行或违反本协议规定，将对第三条（保密信息范围的条款）以及投资、经营、商誉或经济权益产生不利影响，甚至产生直接或间接损害，构成不公平竞争，影响产业公平秩序等，甲方将依据中华人民共和国相关法律、法规等追究其相应法律责任。

**第二条** 术语定义

本协议所称商业秘密，是指企业在生产经营过程中形成的不为公众所知悉，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。

**第三条** 保密信息的范围

经双方确认，乙方在甲方任职期间，因履行职务已经或将要接触或知悉甲方的商业秘密，包括但不限于以下内容：

（1）甲方的客户、员工、管理人员及顾问的名单、联系方式及其他相关信息，包括但不限于姓名、联系电话（移动和固定电话）、电子邮件地址、即时通讯方式或社交网络地址（QQ、MSN、Skype、微信、易信、来往、Line、微博、空间等）、家庭地址等任何足以识别、联系客户、员工、管理人员及顾问的信息；

（2）与甲方经营活动有关的合同文本及法律文书；

（3）甲方经营活动中涉及的关键价格信息；

（4）甲方日常经营管理中的会议决议、会议纪要、谈判与磋商细节等资料；

（5）甲方的具体经营状况及经营策略（如营业额、销售数据、负债、库存、经营方针、投资决策意向、产品定价、服务策略、市场分析、广告策略、定价策略、营销策略等）；

（6）与甲方资产、财务有关的信息（如存货、现金等资产的存放地、保险箱密码、数量、价值等，以及财务报表、账簿、凭证等）；

（7）与甲方人事、管理制度有关的资料（如劳动合同、人事资料、管理资料、培训资料、工资薪酬及福利待遇资料、奖惩情况等）；

（8）甲方的知识产权、专有技术等信息（如产品设计、产品图纸、生产制造工艺及技术、计算机软件程序、数据库、技术数据、专利技术、版权信息、科研成果等）；

**图 A.1 商业秘密保密协议**（续）

（9）根据法律、法规规定以及本协议约定需要保密的其他与技术和经营活动有关的信息。

**第四条** 保密信息的例外

1、在披露时或披露前，已为公众所知晓的信息或资料；

2、能证明从甲方获得相关信息时乙方已经熟知的资料或信息；

3、由第三方合法提供给乙方的非保密资料或信息；

4、未使用甲方的技术资料，由乙方在日常业务中独立学习或研究获得的知识、信息或资料。

**第五条** 保密义务的期限

本协议的有效期为本协议签订之日起至双方解除或者终止劳动关系后___年止。其中涉及国家机密的，依照《中华人民共和国保守国家秘密法》及相关法律法规的规定执行。

**第六条** 保密义务的效力

乙方确认，在与甲方的劳动关系存续期间，需在任何地域内遵守本协议约定之保密义务。乙方不得以该地域不能够或者不具备形成甲方的实际竞争关系为理由，要求甲方排除本协议约定之保密义务。

**第七条** 积极保密义务

1、如乙方须对外使用甲方所披露的信息时，不确定该信息是否为保密信息，需向甲方书面征询，由甲方给予书面答复。

2、乙方应自甲方按要求向其提供保密信息之日起，对相关信息予以保密，不得向任何第三方披露上述信息。

3、为使乙方更好地履行本协议约定之保密义务，甲方应该对乙方进行保密教育及培训。

**第八条** 消极保密义务

1、乙方于任职期间或离职后所知悉、接触、持有、使用之机密资料及密码，系甲方或其客户赖以经营之重要资产，乙方应以善良管理人的注意义务采取有效的措施保护该机密资料及密码，且乙方于任职期间或离职后均不以任何方式泄露或将该机密资料及密码交付给第三人。

**图 A.1 商业秘密保密协议**（续）

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/996041124155010213