ICS 03.100.01
CCS A 01

上海市奉贤区标准化指导性技术文件

DB31-120/Z 011—2024

企业商业秘密管理规范

Management specification for trade secrets of enterprise

2024-04-01 发布　　2024-04-01 实施

上海市奉贤区市场监督管理局　　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。

本文件由上海市奉贤区市场监督管理局提出、归口并组织实施。

本文件起草单位：上海市奉贤区市场监督管理局、上海质量教育培训中心有限公司。

本文件为推荐性。有关对本文件的建议和意见，向奉贤区标准化管理部门或市标准化管理部门反映。

企业商业秘密管理规范

1 范围

本文件规定了企业商业秘密管理的基本要求、定密与解密、商业秘密保护范围、商业秘密保护管理、维权、监督检查和改进要求。

本文件适用于上海市奉贤区化妆品、生物、医药、医疗器械、新材料、新能源、化工、半导体、芯片等企业开展商业秘密管理工作。

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

商业秘密 trade secret

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 carrier

以文字、数据、符号、图形、图像、视频、音频等方式记录和存储商业秘密的介质及其信息。

注：涉密载体通常包括纸质文件、存储介质（磁性介质、光盘、U盘、硬盘、服务器等），以及涉及商业秘密的电子数据。

3.3

涉密物品 secret items

含有商业秘密信息的设备、软件、原材料、半成品、样品、模具、压铸件等。

4 基本要求

4.1 管理职责

4.1.1 最高管理者

为实施商业秘密管理，并持续改进管理的绩效，最高管理者（法定代表人或企业实际控制人）应履行以下职责：

a) 独立行使企业商业秘密管理的最高权力；

b) 指导并支持建立、完善商业秘密管理制度；

c) 确保商业秘密管理工作融入企业的经营管理，并得到有效开展；
d) 确保商业秘密保护资源的配备，所需经费得到财务保障；
e) 分配商业秘密管理职责和权限，确定商业秘密管理部门及其负责人；
f) 对阻挠、干涉商业秘密合规官、保密员等管理人员独立开展商业秘密管理工作的事项进行授权处理；
g) 对商业秘密定密、解密事项进行审批。

4.1.2 管理部门

企业应设立商业秘密管理部门或者依托相关部门开展企业商业秘密管理工作，履行以下职责：
a) 策划、管理企业商业秘密保护系统，并向企业最高管理者报告；
b) 起草、发布商业秘密管理所需的规范性文件；
c) 组织识别商业秘密管理中的相关风险，并采取相应的措施；
d) 开展商业秘密定密、解密日常管理工作；
e) 对商业秘密信息、涉密物品、涉密载体、涉密部门、涉密人员、涉密区域等进行识别和管理；
f) 定期测评企业商业秘密保护现状，并形成书面报告；
g) 组织保密宣传，对员工进行保密培训和考核，提高员工保密意识；
h) 组织对企业商业秘密管理工作进行日常监督检查；
i) 组织对涉嫌侵犯商业秘密的违法犯罪行为进行调查取证和依法维权工作。

4.1.3 相关部门

企业商业秘密管理相关部门负责本部门有关商业秘密的管理工作，包括：
a) 根据管理部门安排，完成企业相关涉密内控文件的制定，并组织在本部门的实施；
b) 执行有关法律法规和政策要求、企业的相关管理制度；
c) 对本部门商业秘密管理工作进行自查，针对问题分析原因，采取改进措施。

4.2 管理制度

应建立健全企业商业秘密管理制度，包括但不限于：
a) 商业秘密保护范围管理制度；
b) 技术、生产/服务提供、销售、采购、IT、财务等涉密岗位人员保密培训和考核管理制度；
c) 适用时，涉密配方及其代码、工艺、流程、诀窍等管理制度；
d) 信息安全管理制度（含病毒防范和病毒库升级）；
e) 商业秘密保护情况日常监督检查管理制度；
f) 查漏补缺、持续改进商业秘密管理绩效的管理制度；
g) 商业秘密维权的管理制度。

4.3 管理人员

4.3.1 商业秘密合规官

4.3.1.1 企业宜设立商业秘密合规官，直属企业最高管理者管理，除满足 4.3.2.1 和 4.3.2.3 要求外，还应满足以下要求：
a) 本科及以上学历，法律专业或其他相近专业；

b) 具有较强的语言交流、沟通和协调能力；
c) 接受过企业商业秘密专业化、系统化培训，具备商业秘密管理能力。

4.3.1.2 企业商业秘密合规官应履行以下职责：
a) 贯彻执行商业秘密保护有关法律法规和其他要求，执行最高管理者的决定；
b) 配备专（兼）职人员负责商业秘密管理工作；
c) 组织开展企业商业秘密定密、解密管理工作；
d) 组织开展企业商业秘密保护制度执行情况的监督检查，对违反制度的行为做出处理决定，并督促责任部门或员工整改；
e) 组织对擅自进入涉密区域、拍照、摄像、使用保密设备、使用保密原材料等行为进行调查和处理；
f) 协助市场监督管理部门调查涉嫌侵犯商业秘密的行为，协助公安机关侦查涉嫌侵犯商业秘密犯罪的行为；
g) 对侵犯企业商业秘密的行为，组织、协调相关部门向人民法院提起诉讼；
h) 适用时，履行企业股东会、董事会(执行董事)、商业秘密保护委员会、商业秘密保护委员会主任授予的其它职权。

4.3.2 商业秘密保密员

4.3.2.1 企业应根据需要配备专职或兼职商业秘密保密员（以下简称“保密员”），满足以下要求：
a) 熟悉商业秘密保护有关的法律法规和其他要求；
b) 接受过商业秘密管理、侵权调查取证、商业秘密维权等专业知识培训，具备相应的工作能力；
c) 保密意识强，工作责任心强，具有较强的执行力；
d) 恪守职业道德，对企业忠诚。

4.3.2.2 保密员应履行以下职责：
a) 组织开展保密相关知识培训和考核工作，增强员工保密意识和责任心；
b) 对使用企业商业秘密事项进行登记、审核等管理；
c) 依授权受理涉嫌侵犯商业秘密的举报，接待举报单位或个人，并为其保密；
d) 对涉嫌侵犯企业商业秘密的行为进行询问、调查；
e) 保密档案的移交、接交和管理；
f) 监督检查企业商业秘密管理制度的执行情况，督促责任部门针对存在问题采取改进措施；
g) 配合管辖地市场监督管理部门调查涉嫌侵犯商业秘密的行为，配合公安机关侦查涉嫌侵犯商业秘密犯罪行为。组织、协调相关部门对侵犯商业秘密的行为向人民法院提起诉讼；
h) 企业明确的其他商业秘密管理职责。

4.3.2.3 保密员应遵循以下行为准则：
a) 遵守企业商业秘密管理制度，自觉履行保密义务；
b) 不滥用职权、玩忽职守或徇私舞弊；
c) 不包庇、放纵侵犯商业秘密行为。

5 定密与解密

5.1 定密

5.1.1 企业可根据自身实际设定商业秘密级别，商业秘密宜分为核心商密和普通商密两个级别，级别

划分和密级期限确定按以下要求：

a) 一旦泄露会给企业造成重大经济损失或削弱竞争优势的信息定为核心商密，期限为10年以上至30年，根据实际确定具体期限；

b) 一旦泄露会给企业造成经济损失的信息及尚未进行定密，但属于不为公众所知悉的涉及企业商业秘密的信息为普通商密，期限为10年（含）以下。

5.1.2 对于以数字化形式存储的数据，企业应发布内部管理文件，根据数据属性（如财务数据、消费者数据、生产数据、研发数据等）对数据规定相应的密级。

5.1.3 企业应对载有商业秘密的文件、资料进行定级，宜采用依次由密级、“★”、保密期限组合的方式进行标识。

示例：如核心商业秘密密级期限为30年，标识为“核心商密★30年”。

5.1.4 企业技术信息、经营信息中属于国家秘密的，应按照国家秘密保护要求进行保护。

5.2 解密

企业商业秘密出现下列情形时，可予以解密。

a) 专利已被授权的。

b) 已经公开的（含互联网公开发布的）。

c) 发表论文、文章的。

6 商业秘密保护范围

企业应根据生产、经营实际明确商业秘密保护范围，包括涉及的技术信息和经营信息。可参考表A.1确定企业商业秘密保护范围内容，规定相应的密级。

7 商业秘密保护管理

7.1 人员管理

7.1.1 员工入职

7.1.1.1 新入职员工、在职员工，应签订商业秘密保护合同（或保密协议，或保密条款），约定商业秘密保护内容。商业秘密保护合同示例见附录B。

7.1.1.2 企业宜与职业经理人、技术人员、销售人员、采购人员、高级管理人员及其他负有保密义务的人员等涉密重点岗位员工签订竞业限制协议，约定竞业限制内容，协议示例见附录C。

7.1.1.3 招聘优秀人才、涉密重点岗位员工，入职前宜开展背景调查、核查，包括查验有无犯罪记录、人民法院执行信息等。

7.1.2 员工培训

7.1.2.1 员工保密培训应列入年度培训计划，应在培训结束后对培训的有效性进行评价，评价结果存档。

7.1.2.2 应对新入职人员进行商业秘密保护培训，内容包括但不限于保密知识培训、视频案例培训、公众号宣传培训等。可采取发放资料、线下集中培训、在线培训或其组合的方式进行商业秘密保护培训，保存培训记录。

7.1.3 员工行为

7.1.3.1 企业员工应遵守商业秘密保护管理制度，履行以下职责：

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

7.1.3.2 企业员工未经书面批准，不准许出现的行为包括但不限于：

a) 登陆未授权账户；
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) 将涉密信息（包括图纸、配方、工艺、流程、源代码、计算机程序及其文档、电子文档、电子数据等）保存在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，包括上传互联网进行公开、微信发送朋友圈等。

7.1.3.3 高层管理人员、中层管理人员中涉及商业秘密的重要岗位人员未经书面批准，不准许出现的行为包括但不限于：

a) 兼职或入股与所在企业经营相关、相同或相似的企业；
b) 与所在企业有交易关系、竞争关系或与行业相同或相似的国内外企业进行联系、签约、交易、结算等行为；
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、业务。

7.1.4 员工离职

7.1.4.1 离职员工应主动移交商业秘密及所有涉密载体和物品，包括但不限于：

a) 涉密文件资料、电子数据及其载体、物品；
b) 账户信息，如账号、密码；
c) 工作电脑、工作手机；
d) 门禁卡、工作服、企业标志牌（如工作证、胸牌）等。

7.1.4.2 可进行离职检查，检查以下内容。

a) 工作电脑数据是否完整，是否被删除。
b) 工作账户：
   1) 近期是否有异常操作，如异常查询、下载、拷贝、修改、删除等；
   2) 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等。

7.1.4.3 宜通过离职谈话，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、使用商业秘密等。

7.1.4.4 应及时通知与离职员工有关的供应商、企业客户、合作单位等，进行业务交接工作。

7.1.5 外部人员来访

7.1.5.1 应限制外来人员访问、参观、考察涉密区域，确因工作需要进入涉密区域的，应经审批，佩戴访客证件，进行进出登记。
7.1.5.2 来访人员经批准进入涉密区域，受访部门应安排人员陪同，不准许来访者使用具有拍照、录音、摄像、信息存储等功能的设备。

7.1.6 相关方合作

7.1.6.1 宜与供应商、客户、合作方签订保密合同或协议，约定保密范围和时效及保密责任和义务、违约责任、管辖权等条款。
7.1.6.2 外聘或委托的专家、顾问、翻译、律师等可能接触涉密信息的外部人员，宜签订保密协议。
7.1.6.3 涉及商业秘密的会议或其他活动，应采取保密措施，包括但不限于：

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。

7.2 生产经营过程管理

7.2.1 技术研发

7.2.1.1 企业宜对从事技术、研发工作的员工进行登记管理，在技术研发部门、实验室、试样室、检测室、样品室等保密区设立门禁系统、监控系统，无关人员不应擅自进入。
7.2.1.2 涉密配方应使用代码，技术研发部门应负责配方及其代码归口管理工作，包括物料代码拟定、完善、配方及其代码的增/删/改、配方及其代码问题收集汇总、协调处理。技术研发部门应确定每个物料的品控检测，确定相关检测的指标、方法。
7.2.1.3 技术研发部门应对实验、试验、检测、小批量生产、大批量生产等涉密情况进行登记和记录，内容宜包括员工姓名、记录时间、存档时间、存档人、参与活动名称（实验、试验、检测、小批量生产、大批量生产）、活动类型、仪器和/或设备、过程、结果、改进意见、相关员工签名、审核人签名。承办人员应在实验、试验、检测、小批量生产、大批量生产之日起每天将当日应存档的记录移交给保密员管理，保密员在收到记录之日起 5 个工作日内移交档案室进行存档管理。没有建立档案室的，由保密员存档管理。
7.2.1.4 不准许任何人将实验、试验、检测、小批量生产、大批量生产等涉密情况在非工作环境下进行记录或保存。承办人员应在工作电脑上建立电子文档，用于日常工作。
7.2.1.5 不准许任何人有拍照、摄像、记录、篡改、毁坏、私自保存等行为。
7.2.1.6 企业宜建立涉密样品室，通过门禁系统和监控系统进行管控，不准许无关人员进入。应明确专人管理工作职责，实施样品的登记管理、领用管理等保密管控措施。

7.2.2 采购

7.2.2.1 企业应对采购供应商、合作企业等进行商业秘密保护现状调查，使外部提供的产品和服务满足商业秘密保护需求。
7.2.2.2 采购的涉密原材料、物料宜实行代码化管理，入库与使用由专人管理。
7.2.2.3 在与采购供应商、合作企业签订的合同中，宜约定商业秘密保护要求，或与采购供应商、合作企业单独签订保密合同或协议。

7.2.3 生产

7.2.3.1 企业应对生产和服务提供的过程(如计划管理、工艺管理、质量管理、成本控制等活动)进行商业秘密保护现状测评，根据结果可划定商业秘密保护重点区域，设立保密标志，宜实行物理隔离保护。涉密区域宜安装监控设备、人脸识别系统，电脑宜安装保密软件。
7.2.3.2 企业应实施生产涉密管控，生产部门指定专人对到厂的涉密物料（包括半成品、零部件、包装材料等）进行校对、接收，按照技术研发部门要求对需要检测的涉密物料进行进出库检测，实施涉密物料的库存管理。

7.2.4 销售

7.2.4.1 应及时将企业的客户或已采集的潜在客户的信息建档管理，避免客户信息外泄、损毁或遗失。涉密文件、资料应指定保密员（或档案管理人员）根据企业的档案管理规定进行保管、使用，并落实必要的保密措施。
7.2.4.2 宜搭建线上的客户管理系统，对客户信息的采集、输入、使用和注销等进行全生命周期的管理，并通过设置系统登陆权限、数据访问权限、数据处理权限等落实保密措施。

7.2.5 交付

应对交付产品/服务过程活动(如包装、仓储、物流配送等)的实施情况及其结果采取措施，满足交易双方对商业秘密保护的需要。

7.2.6 售后

应对售后服务(如服务终端管理、人员培训、售后技术支持、申投诉处理等)及其结果采取措施，满足交易双方对商业秘密保护的需要。

7.3 涉密区域管理

7.3.1 应识别涉密区域，在入口和出口醒目位置张贴保密标志，包括涉密会议室和涉密档案、涉密载体、涉密物品的存放地点及以下可能涉密的区域：

a) 技术、研发、设计、实验室、检测室、样品室、仓库、车间、采购、销售、信息安全管理、IT、财务、证券、统计、审计、合规、监察、纪检等部门；
b) 计算机机房、控制中心、服务器机房等。

涉及国家秘密的涉密区域标识，按照国家有关规定执行。

7.3.2 企业涉密区域应实行进出登记和保密告知管理，并满足以下要求：

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) 限制使用具有录音、摄像、拍照、信息存储等功能的设备；
d) 必要时采取网络隔离阻断等。

7.3.3 企业宜在涉密区域内设置宣传标语等，营造保密氛围。

7.4 涉密信息管理

7.4.1 涉密纸质文档管理

7.4.1.1 涉密文件、资料应有密级、保护期限等标识，归档存放。企业未建立档案室的，应由保密员存档管理。应采取措施防止档案受潮、受损、灭失等情况发生。
7.4.1.2 涉密文件、资料应由部门保密员登记造册，按权限使用，查阅、借阅、续借应进行登记。

7.4.1.3 涉密文件、资料应存放在涉密区域内，复制（复印、打印、扫描、摘抄等）、向第三方披露或使用前应履行审批和登记手续。打印、复印、扫描、查阅、借用等使用涉密文件、资料应由专人管理并登记。

7.4.1.4 企业应配备打印管控系统管理涉密文件、资料的打印、复印、扫描，并保留记录及备份。打印、复印、传真涉密文件、资料时，应具备授权并在机器旁守候及时取走文档。扫描涉密文件、资料不应使用公共盘存储。

7.4.1.5 涉及商业秘密内容的新闻、论文、专利申请等信息发布和公开时，应事先申报，获得书面批准。

7.4.1.6 废弃的涉密文件、资料应按照 7.4.1.7 规定方式销毁，不应随意丢弃。

7.4.1.7 如需销毁涉密的文件、资料（含复制的文件、资料），应由商业秘密管理部门提出申请，商业秘密合规官审核，法定代表人或其授权人批准。可采取的销毁方式包括但不限于：

a) 粉碎成颗粒状；
b) 保密员列出销毁清单，在不少于 2 名员工见证下烧毁。

7.4.2 涉密电子数据管理

7.4.2.1 企业宜定期对涉密电子数据进行备份，妥善保存备份数据。

7.4.2.2 员工需要超出权限查阅或使用涉密数据时，应经书面批准，并在查阅或使用完成后，删除查询或使用过程中产生的备份文件，不准许非工作需要而使用。

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

7.4.2.4 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。对外发送涉密电子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。

7.4.2.5 通过邮件发送涉密电子数据时，应设置加密，可限定文档打开次数、打开时限和编辑权限等。

7.4.2.6 应对涉密电子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。

7.4.2.7 应针对涉密设备、系统开展账户、密码信息的收集、存放和传输的安全管理工作。

7.4.2.8 企业应进行网络信息安全管理，执行病毒防范和病毒库升级等管理制度。

7.4.2.9 应定期进行电脑、系统等安全检查，发现漏洞及时修补。

7.4.3 涉密账户管理

7.4.3.1 应对终端设备、数据库和各类应用系统及其账户实行权限管理，依据岗位职责或特定工作事项按“最小够用”原则设定权限。

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

7.4.3.2 权限到期、人员转岗、项目或事项变更时应重新授权。人员离职时应收回相应权限。

7.4.3.3 各类终端设备、数据库和应用系统应设有账户和密码，不应使用默认密码，不准许保存密码自动登陆。根据业务类型，采取账户、密码管理方式，包括但不限于：

a) 限制使用简单密码；
b) 不定期更改密码；
c) 输错密码三次，锁定账户。

7.5 涉密载体、物品管理

7.5.1 电脑

7.5.1.1 宜将企业涉密电脑中的电子数据存储在内部云服务器上。企业需要存储在涉密电脑本地存储的，宜安装保密管理软件。
7.5.1.2 应关闭或禁用涉密电脑的移动存储、光驱、蓝牙、无线网卡等数据传输功能，以及摄像头、声卡、话筒等音视频采集设备，未经书面许可不准许使用。
7.5.1.3 涉密电脑硬件的配置、维修、报废应经过审批或授权交由指定人员处理，应使用封条封住主机以防止员工私自拆机维修、更换、增加硬件配件。
7.5.1.4 涉密电脑的网络接入、网络配置应按规定设置，不应接入非授权网络。
7.5.1.5 涉密便携机应设置身份验证、硬盘口令、封闭摄像头和麦克风功能，存放时使用带锁的保密柜。
7.5.1.6 不宜在涉密区域使用便携机办公。

7.5.2 智能手机

7.5.2.1 企业宜配置工作手机，用于日常商业秘密管理。
7.5.2.2 涉密区域内不宜使用智能手机。如工作需要确需携带智能手机进入涉密区域，应关闭或禁用摄像头、麦克风，不应在涉密区域内拍照、录音、摄像、设置热点。

7.5.3 产品

7.5.3.1 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，出入口配备摄像监控装置，携带外出时应采取包装等保密措施。
7.5.3.2 涉密项目的不良品应交由专人处理或报废，不应随意丢弃。
7.5.3.3 涉密产品、半成品、原料等的标签应替换为企业内部的编码统一管理。

7.5.4 模具和压铸件

企业应对研发所需的涉密模具、压铸件和/或企业生产所需的模具、压铸件的设计、图纸、工艺、流程、技术参数、文档等信息采取相应保密措施。

7.5.5 移动存储介质

7.5.5.1 未经审批不应使用移动存储设备存储商业秘密信息。涉密移动存储介质不应连接非涉密或未采取保密措施的计算机及电子设备。
7.5.5.2 涉密移动存储介质应由专人管理，且使用身份识别、内容加密、设备绑定等保密措施。

7.6 商业秘密存证管理

7.6.1 企业宜进行商业秘密存证，采取商业秘密保护过程留痕管理，使用区块链技术进行哈希值存证。
7.6.2 企业可以向司法鉴定机构申请出具商业秘密司法鉴定意见书，作为证据提供给管辖地的市场监督管理部门、仲裁机构、公安部门、人民法院。

7.7 商业秘密保护保险

7.7.1 企业宜投保保险公司依法获批的商业秘密保护类保险，企业可选择基础保障、综合保障、全面保障等保险类型之一进行投保。
7.7.2 企业商业秘密被侵犯后，已取得生效的行政处罚决定书或调解书、裁决书或法院判决书的，应按照保险合同约定申请理赔，降低商业秘密维权成本。

7.8 商业秘密合规风险管理

7.8.1 企业宜通过设立举报电话、电子邮箱等方式，鼓励员工对实际存在的问题和商业秘密合规风险进行提示、举报。

7.8.2 企业宜为供应商、委托生产商等第三方开设举报、投诉通道，重点收集本企业商业秘密被侵犯的风险、线索。

8 商业秘密维权

8.1 应急处置

8.1.1 企业宜制定商业秘密泄密紧急处置预案，建立内部应对流程。

8.1.2 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，发现问题及时报告。

8.1.3 出现商业秘密泄露迹象时，企业应：

a) 紧急处置，防止信息扩散；
b) 启动对商业秘密泄露的内部调查取证、评估，查明原因，明确责任；
c) 采取措施，对商业秘密泄露的危害进行控制，减少损失。

8.2 证据搜集

8.2.1 发现商业秘密涉嫌被侵权时，应搜集并整理下列证据、材料：

a) 企业是该商业秘密的权利人的证据，包括：
   1) 已采取的相应商业秘密保护措施；
   2) 企业认为是商业秘密的书面证据和证实性材料。
b) 企业商业秘密被侵犯的初步证据，包括：
   1) 涉嫌侵犯商业秘密人员的姓名、性别、年龄、地址、照片等基本信息，涉及第三人的，提供涉嫌侵犯商业秘密的企业名称、地址、法定代表人、注册登记情况等信息；
   2) 涉嫌侵犯商业秘密人员签订的劳动合同、商业秘密保护合同（或保密协议，或保密条款）、竞业限制协议、参与保密培训记录、具体工作职责等信息；
   3) 涉嫌侵犯商业秘密人员能够接触商业秘密的证据；
   4) 相关涉嫌侵犯商业秘密的证据。
c) 该商业秘密被侵犯的事实，包括：
   1) 侵权行为具体表现（如披露、使用等）；
   2) 商业秘密被侵犯所受的损失。

8.2.2 发现商业秘密涉嫌被侵权时，可向商业秘密保护服务机构寻求帮助。可向商业秘密鉴定机构办理商业秘密的非公知性、同一性的鉴定，向评估机构办理损失评估报告。

8.3 维权途径

企业商业秘密涉嫌被侵犯时可依法通过下列途径进行维权：

a) 向管辖地的市场监督管理部门举报投诉；
b) 向管辖地公安机关控告；
c) 向管辖地的劳动仲裁委员会申请劳动仲裁；
d) 向管辖地的仲裁委员会申请仲裁；

e） 向管辖地的人民法院提起民事诉讼；
f） 向管辖地的人民检察院申请法律监督等。

9 监督检查和改进

9.1 企业商业秘密管理部门及保密员应采取现场观察、查阅文件和记录、员工访谈等方式开展商业秘密保护的日常监督检查工作，并保存检查记录。宜利用办公系统采取技术措施开展日常监督检查工作。
9.2 企业宜定期对商业秘密保护现状进行测评，对管理情况进行评审，并形成书面报告。
9.3 企业应对日常监督检查、商业秘密保护现状测评、商业秘密管理情况评审等发现的问题进行汇总分析，并采取改进措施，持续提升企业商业秘密管理的绩效。

附 录 A
（资料性）
企业商业秘密保护范围

表A.1给出了企业商业秘密保护范围的参考内容和密级，企业可根据实际选择适用的内容，也可在表A.1给出内容基础上增加其他内容。

表A.1 商业秘密保护范围参考内容及密级

序号	涉密信息	涉密项目	商业秘密保护范围参考内容	参考密级
1	技术信息	设计和生产信息	企业生产、加工、代加工、销售的各种产品的设计、实验、配方、技术数据、技术参数、技术路线、专有技术、图纸、生产工艺、工艺流程、工艺诀窍、制作方法、经验公式、管理诀窍、样品（包括模型）等信息。与技术有关的结构、原料、组分、材料、样品、样式、方法或其步骤等信息	核心商密
2		技术标准	设计、工艺、模具、压铸件、电子数据等相关技术标准	核心商密
3		软件信息	设计、美工、源代码、计算机程序及其文档、算法、算力、电子数据等信息，以及各种软件内的图纸、图形、三维模型、文档、数据、资料等	核心商密
4	经营信息	管理文件	与企业生产经营相关的、限于企业生产经营管理使用的各种制度文件，如办法、规定、流程、要求、指导书、方案、表式等，与企业生产经营相关的各种控制文件，如程序、规程等	核心商密
5		决策信息	策划或营销或投资的调查、策略、方案、计划、步骤等，以及尚未付诸实施的市场预测、经营战略、经营方向、经营规划、经营项目、经营决策等	核心商密
6		研发信息	各类产品（包括部件）科研计划、开发计划、实施进度及其各种文档、数据、过程、结果等信息	核心商密
7		采购加工信息	采购渠道、采购价格、采购方法、成本构成等采购信息。原材料、零部件、半成品、成品的加工、协作等信息	核心商密
8		销售信息	销售渠道、销售价格、销售方法等销售信息；客户名单、客户名片、客户联系方式、客户数据、客户资料、客户关系、交易习惯、客户爱好、客户要求、经营活动材料等	核心商密
9		物流和运输信息	物流合同、运输合同、物品清单、交接材料等信息	核心商密
10		合同及招投标信息	签订的各类合同（包括订单、协议等）及其签订的过程、文件、资料等经营信息，与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料等信息	核心商密
11		产品信息	与企业经营相关联的实验室实验、认证、检测、检验、验资、评估、审计、委托调查、中介服务等文档、数据、文件等信息	核心商密
12		设备（除计算机）信息	涉密设备、生产设备及其相关文档、图纸、数据、资料等信息	核心商密

表 A.1 商业秘密保护范围参考内容及密级（续）

序号	涉密信息	涉密项目	商业秘密保护范围参考内容	参考密级
13	经营信息	计算机信息	计算机设备、计算机数据库、电脑、电脑硬盘、普通U盘、软盘、光盘、网盘、云盘、电子邮箱等载有、存储的信息；电子邮箱、微信、QQ以及其它聊天工具中的用户名、密码及其信息；电子邮件、数据传送、传真、电话通话、手机通话中涉及未披露的商业秘密信息	核心商密
14		人力资源信息	员工劳动合同、商业秘密保护合同（或保密协议，或保密条款）、竞业限制协议及员工、聘用人员的档案资料、数据等	核心商密
15		财务信息	会计凭证、成本计算、成本分析、财务报表、财务分析、统计报表、预决算报告、各类帐册和财务表单等财务信息，财务软件中记载的财务信息	核心商密
16		未披露信息	商业秘密管理部门以及企业各部门商量、商议、洽谈、决定的涉及商业秘密的未披露的信息	普通商密
17	其他	其他信息	企业认为有必要采取保密措施的其他技术信息和经营信息	根据5.1.1规定定密

附 录 B
（资料性）
商业秘密保护合同示例

图B.1给出了商业秘密保护合同内容的示例。

商业秘密保护合同

商业秘密权利人：XXXXXX有限公司 （下称“甲方”）

劳动者或聘用人员：　　性别：　　年龄：　　岁 （下称“乙方”）

身份证号：　　手机：

岗　　位：　　职务：

家庭住址：

现在住所：

乙方知悉甲方是商业秘密权利人，自愿因工作而知悉的商业秘密对甲方承担保密义务，甲、乙双方在自愿、诚实信用原则下，经充分协商，达成如下一致条款，并共同恪守。

一、乙方履行告知义务

乙方承诺进入甲方工作时没有掌握甲方或第三人采取合理的商业秘密保护措施的商业秘密。

二、商业秘密范围

甲方的商业秘密范围是指甲方不为公众所知悉、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。

甲方的商业秘密包括且不限于在发布的《商业秘密保护范围规定》列出的商业秘密保护范围，包括且不限于特定的、完整的、部分的、个别的不为公众所知悉的或未披露的商业信息，包括且不限于涉及商业秘密的草稿、拟稿、草案、样品、图形、模型、文件、数据、资料等商业信息。

三、乙方对商业秘密保护的义务

乙方已充分认识到保守甲方商业秘密是关系到公司生存和发展的重要问题，因此，乙方对甲方的所有商业秘密承担保护义务。

乙方保证严格保守前条所列之商业秘密，因工作需要而经甲方商业秘密保护部批准，向应该知道前条所列之商业秘密内容的甲方客户或第三人进行必要的保密交流除外，乙方：

1、严格遵守甲方制定的涉及商业秘密保护的各项制度；

2、不得在与甲方有竞争关系的企业兼职；

3、不得使第三人获得、使用或计划使用甲方商业秘密；

4、不得直接或间接向甲方内部无关人员泄露；

5、不得直接或间接向甲方外部的单位或人员泄露；

6、不得为自己利益使用或计划使用；

图 B.1 商业秘密保护合同示例

7、不得复制或披露包含甲方商业秘密的文件或文件副本；

8、不得擅自拷贝甲方计算机软件的任何数据、文件资料或信息；

9、对因工作所保管、接触的甲方客户提交的文件应当妥善保管，未经商业秘密保护部批准，不得超出工作范围使用；

10、发现第三人以盗窃、贿赂、欺诈、胁迫、电子侵入或其他不正当手段谋取或计划谋取甲方商业秘密时，立即向商业秘密保护部报告，并积极采取保护的必要措施；

11、其它应当承担的商业秘密保护义务。

四、公知领域排除

前条所列的商业秘密不包括乙方从公知领域已经知悉的信息。若乙方知悉的或从其他渠道获知的，乙方应当在本合同签订之日起____日内或知悉之日起____日内向甲方商业秘密保护部报告名称和来源，并做出详细书面报告。

五、成果归属和报告义务

1、乙方因工作、职务而创造和构思的有关技术和经营的商业秘密或信息归甲方所有；为甲方公司利益而做出职务成果时，应当在做出之日起_____日内向甲方商业秘密保护部报告。

2、对乙方与甲方经营范围有关的非职务发明，甲方有优先受让权，在条件相同情况下，乙方应当将该商业秘密许可或转让给甲方，甲方应当以合适的方式使用或受让，并支付合理的报酬。

3、甲方不实施职务成果，乙方实施又不影响甲方科研、生产、经营利益的条件下，甲方可允许乙方以发包、租赁、接受许可使用、接受转让等方式，开发利用该商业秘密。

4、本条不影响乙方在职期间或离职之后对非职务发明的权利，乙方以书面形式向甲方提交非职务发明的材料，经甲方确认的非职务发明，与甲方无关。

六、职务成果的奖励

甲方制定的职务成果奖励规定，可作为本合同的重要组成部分，并遵照执行。

七、乙方承诺

乙方承诺无论是在甲方工作还是以任何原因离职或解除劳动关系后，不会采取下列方式之一披露、擅自使用或许可第三人使用甲方的商业秘密：

1、将自己使用的电脑用户名、密码告诉第三人；对电脑页面或内容进行拍照、摄像；非法获取电子数据商业秘密；以电子侵入或非法侵入方式使用电脑、获取存储的商业秘密或信息。

2、与跟甲方有交易关系或竞争关系、行业相同或相似的国内外任何企业进行交易，或由亲戚朋友名义进行交易或变相交易。

3、组建、参与组建或投资、变相投资与甲方经营相关、相同或相似的企业。

4、直接、间接或帮助第三人劝诱甲方掌握商业秘密的人员或职员离开甲方；

5、直接、间接试图影响或者侵犯甲方拥有的客户名单及其客户关系的商业秘密，包括客户名称、联系人、联系人习惯、联系方式、聊天工具、电子邮箱、交易习惯、合同关系、合同内容、佣金或折扣、交提货方式、款项结算等。

6、利用非工作时间在与甲方的同行业企业内兼职或变相工作等。

7、采取其他不正当手段。

乙方无论以何种原因离职或解除劳动关系后，仍然无条件地对甲方商业秘密承担保密义务，直至该商业秘密完

图 B.1 商业秘密保护合同示例（续）

全公开。

八、保密材料的交还

乙方无论何种原因离开甲方，均应当自觉办理离职手续、接受甲方组织的离职前保密谈话，并交还甲方《商业秘密保护范围规定》所列之属于甲方商业秘密的所有数据、文件、资料（包括电脑、硬盘、U 盘、光盘、软盘等存储载体中的信息）、物品等；个人工作日记中含有甲方商业秘密的，应当同时交还或在商业秘密保护部监督下销毁。乙方应当有义务列出掌握甲方商业秘密的清单，交商业秘密保护部确认，双方签字，并办理交还的交接手续。

若乙方擅自带走或不予交还的，视为盗窃商业秘密的行为。

九、合同有效期限

1、上述保密义务对乙方长期有效，无论其在职期间，还是离职之后，除非甲方商业秘密为公众所知悉。

2、如果甲方商业秘密进入公知领域，是因乙方的过错，除追究法律责任外，乙方或知悉方仍无权使用该商业秘密。

十、法律责任

鉴于甲方商业秘密被披露、使用或允许第三人使用或转让给第三人将会削弱甲方竞争优势，造成不可估量的经济损失，为了有效保护甲方商业秘密，双方约定若乙方违反本合同规定，乙方应当向甲方支付违约金为_____万元。

十一、特别约定

乙方除遵守甲方建立的商业秘密保护系统各项规章制度外，还应当遵守工作岗位所在的企业建立的商业秘密保护各项规章制度。

十二、本合同在原有保密规定、保密条款上进行完善，本合同成为甲、乙双方签订的劳动合同的重要组成部分；任何一方不得擅自变更或解除，自本合同签订之日起，以前签订的合同或涉及商业秘密保护的条款与本合同有不一致的地方，以本合同为准。

十三、未尽事宜，甲、乙双方友好协商解决；协商不成的，双方约定由上海仲裁委员会仲裁。

十四、本合同一式贰份，甲、乙双方各执壹份，自签订之日起具有法律约束力。

甲方(公章)：　　乙方（签字指印）：

签订日期：　　年　月　日

图 B.1 商业秘密保护合同示例（续）

附 录 C
（资料性）
竞业限制协议示例

图C.1给出了竞业限制协议内容示例。

竞业限制协议

甲方：XXXXXX有限公司

经营地址：

乙方：　　姓名：　　性别：　　身份证号：

居住地址：　　手机号码：

送达地址：

甲、乙双方在自愿、平等、诚信基础上，经过充分协商，签订《竞业限制协议》，达成如下一致条款，双方共同恪守。

一、竞业限制期限

竞业限制期限为贰年，自甲方与乙方劳动关系终止或解除之日起计算。

二、竞业限制补偿金

劳动关系终止或解除之日起，甲方应当在每月____日前向乙方支付竞业限制补偿金，补偿金额按照劳动者在劳动合同解除或者终止前十二个月平均工资的_____计算（工资中不包括：加班费、奖金、分红、股权激励等），按月支付。

三、支付方式

甲方在每月_____日前汇付乙方专设帐户，乙方接收竞业限制补偿金的专设帐户为乙方在甲方工作期间领取工资的银行账户，乙方不得注销。

如因乙方注销领工资的银行卡、拒绝接收竞业限制补偿金等原因而导致甲方未能按期支付的，不影响本竞业限制协议之法律效力。在乙方未能合理配合消除支付障碍之前，甲方有权暂停支付竞业限制补偿金。

四、双方约定

（一）乙方在劳动合同终止或解除之日起贰年内，不得在与甲方生产或者经营同类产品、从事同类业务的有竞争关系的其他用人单位工作，不得自己组建、参与组建生产或者经营同类产品、从事同类业务或为其提供于甲方不利的帮助，不得直接、间接或帮助他人劝诱甲方掌握商业秘密的人员、关键岗位上的人员、熟练操作人员等离开甲方企业，不得违反甲方要求的保密义务。

（二）甲方经通知可以依法解除本协议，本协议自乙方收到通知之日起解除。

（三）乙方应当在离职前向甲方提供书面、有效的联系人、联系电话、地址、微信号、QQ、邮箱等信息，并及时将更新后的信息书面通知甲方。如因乙方原因造成甲方无法通知的，相应的法律责任由乙方承担。

（四）本竞业限制协议是《劳动合同》的重要组成部分，一般情况下与《劳动合同》同时签署并具有同等法律效力；如系事后补签的，自补签之日起生效。

（五）无论本协议中约定的竞业限制补偿金是否最终被认定为有效还是无效，均不会导致本协议其他条款的无效。

图C.1 竞业限制协议示例

五、违约责任

（一）乙方违反竞业限制义务的，应当承担下列违约责任与赔偿责任：

1．乙方在违约之日起 3 日内将已经收到的全部竞业限制补偿金返还给甲方，汇入甲方银行账户（户名：_____、开户银行：_____、账号：_____）。

2.甲方在乙方违约之日起不必支付尚未支付的全部竞业限制补偿金。

3.乙方应当在违约之日起支付违约金_____万元人民币给甲方。如果乙方支付违约金后，甲方要求乙方按照约定继续履行竞业限制义务的，乙方应当无条件地继续履行。

4.乙方支付上述违约金不足以弥补甲方实际损失的，应当另向甲方赔偿经济损失，包括但不限于甲方调查乙方涉嫌违反竞业限制的调查服务费、公证费用、差旅费等合理调查费用，以及律师费、诉讼费、执行费等。

（二）乙方在离职之日起贰年内不得直接、间接或者试图影响甲方拥有的客户关系，包括但不限于原材料、零部件、初级产品、委托加工产品、产品成品等涉及的研发、供应、销售、客服等人员，使其向乙方或第三人转移、发生交易关系。乙方违反本条规定构成违约的，应当向甲方支付违约金_____万元人民币。

六、商业秘密保护

本《竞业限制协议》系甲方的商业秘密，为核心秘密★30 年，已纳入甲方企业商业秘密保护系统进行保密管理，仅限于甲、乙双方知悉；乙方应当承担保密义务，不得披露、使用、许可第三人使用。鉴于甲方商业秘密保护之需要，乙方需要复印、复制、拍照、摄像、扫描、刻录、镜像、截屏、抄摘、转借、传阅、微信或电子邮件发送本协议的，应当事先经甲方书面批准。

七、本协议一式贰份，甲、乙双方各执壹份，自双方签订之日起立即生效。

甲方（公章）：　　乙方（签名）：

签订时间：　　年　　月　　日

图C.1 竞业限制协议示例（续）

参 考 文 献

[1] GB/T 29490—2023 企业知识产权合规管理体系 要求

[2] 中华人民共和国反不正当竞争法

[3] 中华人民共和国刑法[4] 最高人民法院关于审理劳动争议案件适用法律若干问题的解释（四）（最高人民法院 法释〔2013〕4号）

[5] 科学技术保密规定（中华人民共和国科学技术部、中华人民共和国国家保密局2015年11月16日联合发布）

[6] 全国商业秘密保护创新试点工作方案（国家市场监督管理总局 国市监竞争发〔2022〕26号）

[7] 化妆品企业商业秘密合规管理指引（试行）（上海市奉贤区人民检察院、上海市奉贤区市场监督管理局、东方美谷企业集团股份有限公司、上海日用化学品行业协会2023年11月7日联合发布）