企业商业秘密保护工作指南

Guide for the protection of enterprise trade secrets

目 次

企业商业秘密保护工作指南

1 范围

本文件规定了商业秘密保护的基本原则、管理机构和职责、商业秘密事项管理、保密措施、商业秘密维权等内容。

本文件适用于临港新片区企业开展商业秘密保护工作。事业单位、研究机构、社会团体等其他组织机构的商业秘密保护工作可参照本文件执行。

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

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1：“不为公众所知悉”和“具有商业价值”的具体内容见《中华人民共和国反不正当竞争法》第九条第四款的规定。

注2：权利人包括商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。(《中华人民共和国刑法》第二百一十九条)。

注3：“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》。

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。

注：《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》第一条。

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1：客户包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

注2：《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》第一条。

3.4

商业秘密保护 trade secret protection

商业秘密权利人采取合理的步骤以确保其秘密性质的行为。

3.5

涉密载体 secret-related carriers

以文字、数据、符号、图形、实物、视频和音频等形式记载和存储商业秘密的纸介质、光介质、电磁介质等各类物品。

注1：纸介质是以文字、图形、符号记录的各类物品，如文件、资料、文稿、档案、电报、信函、数据统计、图标、地图、照片、书刊、图文资料等。

注2：光介质是以光、电信号记录、传输的各类物品，如 CD、VCD、DVD、电波、光纤等。

注3：电磁介质是以电子介质或磁介质记录的各类物品，如计算机磁盘（软盘、硬盘）、磁带录音带、录像带等。

3.6

涉密物品 secret-related items

直接含有商业秘密信息，或者通过观察、测试、分析等手段能够获取所承载的商业秘密信息的设备或产品、原材料、半成品、样品等。

3.7 **涉密设备** secret-relatedequipment

采集、存储、处理、传输涉及商业秘密信息的各类设备。

3.8

涉密计算机 secret-related computers

生成、储存、处理涉密信息的计算机。

注：计算机是指处理或存储商业秘密信息的台式机、便携机、一体机、平板等各类涉密计算机。

3.9

涉密区域 secret-related area

可以接触到商业秘密信息的一切场所，包括但不限于企业园区、厂房、车间、实验室、办公室、保密室、档案室、机房、用户现场等。

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、规章规定。确保所有的保护措施、管理行为和维权活动都在法律框架内进行。

4.2 限制知悉范围原则

根据管理、科研、业务工作的需要，若员工未获授权掌握特定商业秘密将致使生产、工作难以开展或交易无法达成，则可向相关员工披露商业秘密；严格限定知悉人员范围，确保仅为实际开展工作确有必要了解商业秘密的人员才能获得相关信息，以降低泄密的风险。

4.3 分割原则

把完整的事项根据经营、管理的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，以防止商业秘密的整体泄露，并且便于追踪信息的流向。

4.4 分级管理原则

商业秘密管理工作宜实行统一领导、分级管理、分工负责的领导体制和工作机制。企业最高管理层应当对商业秘密保护负最终责任，而具体的保护工作则由专门的部门或团队执行，并确保每一级管理人员都清楚自己的职责范围。

4.5 预防为先原则

商业秘密保护应以预防为主，通过建立健全商业秘密保护机制和制度，识别和确定商业秘密的泄密风险，加强保密事项的管理，并采取相应的保护和应急措施，预防或避免商业秘密泄密或被侵犯的行为发生。

4.6 依法维权原则

商业秘密受到侵犯时，应理性表达利益诉求，依据相关法律法规的规定，向行政管理机构、公安机关、司法机关等寻求保护，维护自身的合法权益。

4.7 多元协同原则

鼓励利用行业协会、第三方服务机构等多方社会力量提供的宣传培训、技术咨询、法律援助等服务，提升商业秘密保护能力，构建企业内外部相结合的保护体系。

5 管理机构和职责

5.1 基本要求

5.1.1 企业应设立商业秘密保护部门或依托相关部门开展商业秘密保护工作，并配备专（兼）职保密员。

5.1.2 分支机构、子公司和关联企业可参照设置商业秘密保护部门和专（兼）职保密员。

5.1.3 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。

5.1.4 企业对商业秘密的保护实行领导负责制，即最高管理者负最终责任。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。

5.1.5 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。

5.2 领导职责

企业的最高管理者是商业秘密保护的第一责任人，应组织最高管理层通过以下职责进行商业秘密保护活动：

a） 宣传贯彻国家有关商业秘密保护的法律、法规和规章；
b） 制定商业秘密保护方针政策；
c） 建立健全商业秘密组织机构及体系；
d） 决定重大商业秘密事项；
e） 确定商业秘密保护的目标；
f） 明确商业秘密保护的职责和权限；
g） 保证商业秘密保护活动的资源支持。

5.3 商业秘密保护部门职责

企业应建立商业秘密保护部门，并配备专（兼）职保密员，承担以下职责：

a） 拟定商业秘密保护计划并组织实施；
b） 拟定商业秘密保护文件并组织实施，包括商业秘密保护范围、秘密性控制、保密措施运用的策划与管理、商业秘密处置与奖惩等；

c） 建立、实施和运行商业秘密管理体系，向最高管理层提出商业秘密保护体系的改进需求建议；
d） 识别和管理商业秘密事项、涉密部门、涉密人员、涉密区域；
e） 组织企业员工进行商业秘密保护培训；
f） 负责计算机信息网络、涉密载体、涉密物品的安全保密及管理工作；
g） 履行商业秘密泄露的证据整理、搜集、举证、协助调查取证等工作。

5.4 业务部门职责

业务部门应承担以下职责：
a） 企业应指定各业务部门的管理者作为各业务部门商业秘密管理的责任人；
b） 在重点业务部门配备专（兼）职保密员，负责各自范围内企业的生产、经营等商业秘密的保护。

5.5 专（兼）职保密员职责

专（兼）职保密员应承担以下职责：
a） 宣传商业秘密保护的意义、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。

6 商业秘密事项管理

6.1 定密

6.1.1 不应作为商业秘密的情形

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） 可通过无需额外特殊授权或付费获取限制的合法渠道获得的信息；
j） 法律、法规、规章及相关司法解释规定的其他情形。

6.1.2 确定商业秘密的范围

企业应依法确定本企业商业秘密保护范围，宜包括：
a） 技术类涉密信息：
设计信息：与产品或服务有关的程序、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；
生产或服务信息：产品的配方、工艺流程、样式、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；
软件信息：设计计划、设计方案、源代码、算法、编码、网络协议、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，如未公开的专利申报信息等。

b） 经营类涉密信息：
企业基本信息：组织架构、决议文件、内部通知、规章制度、会议纪要等；
决策信息：与经营活动有关的战略规划（计划）、战略决策、投融资决策、商业模式、研发策略、管理方法、项目投资策略及方案、专利规划布局、产权交易、股权激励方案等；
经营信息：产购销计划（方案）、产购销协议、招（投）标标书、产购销记录（订单）、运营成本、内部定价文件、产品合格率、库存量、创意管理等；
研发信息：研发策略、研发经费预算等；
采购信息：主要供应商信息、进价策略、采购渠道、主要原材料指标、采购计划、采购记录等；
销售信息：营销计划、营销方案、营销政策、营销手册、销售协议、销售记录等；
财务信息：财务报表、财务分析、统计报表、预决算报告、各类账册、工资信息、银行存款核算、往来核算、成本核算、存货核算、长期投资核算、工资核算、销售核算、所有者权益核算、外部会计报告、内部会计报告、股权调整方案、对外交流和商业谈判摘要等；
供应商和客户信息：供应商/客户名称、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、企业技术合作方案、企业突发事件处置方案、企业涉稳事件处置方案、企业突发和涉稳事件处置资料；
其他：企业认为有必要采取保密措施的其他经营信息。

c） 除技术类涉密信息、经营类涉密信息以外，其他符合商业秘密构成要件的商业信息。

6.1.3 商业秘密确定的考虑因素

企业对商业秘密进行确定时应考虑但不限于以下一般因素：

a） 商业秘密信息的经济价值；
b） 产生商业秘密信息投入的成本；
c） 商业秘密信息对企业的重要程度；
d） 商业秘密信息对竞争对手的价值；
e） 因商业秘密信息泄露等可能遭受的损失程度；
f） 商业秘密信息泄露后可能承担的法律责任；
g） 商业秘密信息在企业内部可查阅的范围；
h） 对商业秘密采取保密措施所需的成本；
i） 法律、法规、规章及相关司法解释等规定的其他情形。

6.1.4 商业秘密的分级

根据商业秘密的秘密性和价值性，企业可将商业秘密划分为核心商业秘密、重要商业秘密、一般商业秘密，并实行定期或不定期复评、动态调整：

a） 核心商业秘密是指对企业持续发展和市场竞争力具有决定性影响，公开或泄露后会导致企业遭受无法挽回的损失，甚至威胁到企业生存的信息；

b） 重要商业秘密是指对企业运营和竞争优势有显著影响，公开或泄露后会导致企业遭受重大损失，但不会对企业的生存构成直接威胁的信息；

c） 一般商业秘密是指对企业运营具有一定影响，公开或泄露后会导致企业遭受一定损失，但不会对企业的核心竞争力或市场地位造成重大影响的信息。

6.1.5 商业秘密保密期限

企业可根据商业秘密的密级划分以及商业秘密生命周期、技术成熟程度、潜在价值、市场需求等，确定商业秘密保密期限。可以预见时限的以年、月、日计，不可以预见时限的应定为“长期”或者“公布前”。

6.1.6 商业秘密接触范围

企业应根据商业秘密的内容和密级，确定商业秘密的主责部门与接触范围。

企业应保留接触范围的成文信息。

6.1.7 商业秘密的流转要求

企业应根据商业秘密的内容和密级确定商业秘密的流转要求；通过信息系统或者会议等形式发布时，应采取签字或者数字化身份认证等方式记录接触范围。

企业应保留商业秘密流转的成文信息。

6.1.8 商业秘密的存证

企业应根据涉密载体管理条件、商业秘密的密级与载体情况确定合适的存证方式：

a） 对于商业秘密所涉及的文件，企业应通过编校审等书面签字审核流程或带有时间戳的电子审核流程，使之成为受控文件；

b） 企业可将必要且适当的涉密载体委托第三方机构进行存证。第三方机构应为具有一定社会公信力的、独立的、经相关司法机关认可的法人主体。商业秘密存证的信息载体可以是报告、论文、图纸、磁带、磁盘等信息化载体，也可以是样品、样机等物化载体。

6.1.9 商业秘密清单

企业应形成商业秘密清单，内容可包括商业秘密主题、密级、保密期限、主责部门、接触范围、流转要求、保存方式、存证方式等。

6.2 隐秘

6.2.1 下列情形涉及商业秘密的，应对相关信息予以隐藏：

a） 与供应商、客户、合作方等相关方的沟通和信息往来中；

b） 信息公开、发布、流转时；

c） 协助其他相关方尽职调查时；

d） 其他情形。

6.2.2 配合行政机关和部门的行政检查、行政执法行动中，涉及隐秘事项检查的，企业应主动提醒

执法检查人员履行保密义务。

6.2.3 可采取的隐藏方式为：

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。

6.3 解密

6.3.1 企业的商业秘密出现下列情形时，可予以解密：

a） 企业认为商业秘密已不再具有保护价值的；
b） 保密期限届满的；
c） 其他因素导致商业秘密被公开的。

6.3.2 可采取的解密方式一般包括：

a） 移出涉密区域；
b） 消除或变更密级标识、提示；
c） 电子文档解密；
d） 发文公布；
e） 其他方式。

6.3.3 保密期限内解密的，应以能够明显识别的方式标明“解密”的字样。

6.4 变更

6.4.1 企业的商业秘密出现下列情形时，应及时变更：

a） 因工作需要或人员变动，知悉范围有较大变化的；
b） 因法律法规或政策改变，商业秘密级别出现变化的；
c） 保密期限已经发生变化的；
d） 商业秘密泄露后对企业利益的损害程度发生变化的。

6.4.2 变更流程如下：

a） 商业秘密业务部门向商业秘密保护部门提交商业秘密变更申请；
b） 商业秘密保护部门对商业秘密进行评估审核；
c） 商业秘密级别和保密期限变更后，商业秘密相关部门应及时变更标识。

6.5 销毁

6.5.1 销毁涉密资料、涉密载体和涉密物品，应由专（兼）职保密员列出销毁清单，经商业秘密保护部门审批后实施。

6.5.2 销毁过程宜采取下列方式进行监督管理：

a） 在视频监控范围内销毁；
b） 在不少于2名专（兼）职保密员见证下销毁；
c） 对销毁过程录像、记录等。

6.5.3 应采取合适的方式妥善销毁涉密资料和涉密物品，包括：

a） 纸质类资料作粉碎性或焚烧处理；
b） 电子信息应利用专业的数据擦除软件彻底删除，或采用物理破坏储存介质的方式作销毁处理；
c） 含有核心商业秘密的电子信息载体应采用物理破坏储存介质的方式作销毁处理；

d） 其他合适的方式。

7 保密措施

7.1 保密教育

7.1.1 培训计划与目标

7.1.1.1 企业应将商业秘密保护培训列入年度培训计划，开展全员保密知识普及。组织不同涉密岗位人员分别参加有针对性的保密教育培训，并保存培训记录。

7.1.1.2 商业秘密保护教育应促使在职员工对商业秘密可能泄露的异常状态及承担的法律后果保持足够警觉。

7.1.2 培训组织方式及对象

7.1.2.1 企业商业秘密保护部门负责组织对中层领导及各部门保密员开展培训教育,各部门再进行内部培训，采用横向纵向相结合的方法，实现全员保密教育，增强保密意识。

7.1.2.2 对新入职员工开展保密培训；定期对全体员工开展保密培训；对重点岗位的涉密人员定期开展专项保密培训。

7.1.3 保密培训内容与形式

7.1.3.1 企业对员工开展保密培训的内容应包括但不限于以下内容：

a） 商业秘密对企业的重要性；
b） 商业秘密的定义以及作为企业职务成果的属性；
c） 可能导致商业秘密泄露的行为和潜在风险；
d） 侵害商业秘密可能承担的法律责任，包括民事赔偿、刑事处罚等；
e） 企业的商业秘密管理制度及相关流程；
f） 其他与保密义务、保密范围、保密行为有关的内容。

7.1.3.2 保密培训可采用线下、线上集中培训，或录制成视频、音频课程等形式。

7.1.4 保密宣传教育

企业可通过以下方式开展保密宣传教育：

a） 发放员工手册；
b） 定期线上推送保密宣传案例；
c） 组织知识竞赛；
d） 利用办公环境展示宣传材料、播放宣传视频；
e） 定期召开全员保密动员大会。

7.1.5 考核与激励

7.1.5.1 定期组织员工进行商业秘密保护知识考核，考核结果纳入员工个人档案。

7.1.5.2 考核结果与员工绩效奖挂钩，对表现优秀的员工给予奖励，对考核不合格的员工进行培训指导和必要的处罚。

7.1.5.3 根据考核结果，不断优化宣传、培训内容，提高培训效果。

7.1.6 记录与存档

7.1.6.1 所有培训活动应做好详细记录，包括参与人员名单、培训内容概要、时间地点等信息。

7.1.6.2 记录应妥善保存，作为持续改进培训计划的基础资料。

7.2 奖惩

7.2.1 奖惩制度建立

企业应依法建立商业秘密保护奖惩制度，明确奖励与处罚的具体规定。奖惩制度应包括对员工在保守商业秘密方面的忠诚行为给予奖励，以及对违反商业秘密管理规定的行为进行处罚。

7.2.2 奖励措施

7.2.2.1 对于依照企业规定，在保守商业秘密方面表现突出的员工，应予以表彰和奖励，具体包括：

a） 忠于职守，从事保密工作取得显著成效；

b） 发现他人泄密后，及时采取补救措施，避免或减轻损害后果；

c） 对泄密或者非法获取商业秘密的行为及时检举；

d） 发现企业商业秘密管理体系、措施、技术手段存在漏洞，并提供有效线索或改进意见。

7.2.2.2 予以表彰和奖励的方式，具体为：

a） 根据员工的表现和贡献，给予物质奖励、精神鼓励或职位晋升；

b） 对采纳的线索或意见，根据其贡献度给予相应的奖励。

7.2.3 处罚措施

7.2.3.1 企业应参照有关法规并依据建立的奖惩制度，对违反企业商业秘密管理规定的员工进行处罚，违反企业商业秘密管理规定的具体行为包括：

a） 不遵守企业商业秘密管理规定，导致泄密事件；

b） 故意或过失泄露企业商业秘密；

c） 非法获取、使用或披露企业商业秘密；

d） 其他违反商业秘密管理规定的行为。

7.2.3.2 予以处罚的方式，具体为：

a） 根据违规行为的严重程度，给予警告、记过、降职、降薪等纪律处分；

b） 对于严重违规行为，可依法解除劳动合同；

c） 涉嫌犯罪的，移交司法机关追究法律责任。

7.2.4 奖惩程序

7.2.4.1 奖励与处罚的决定应基于充分的事实调查和证据支持。

7.2.4.2 处罚结果应形成书面文件，并在企业内部进行通报，同时存档备查。

7.2.4.3 奖励与处罚的决定应遵循公平、公正、公开的原则，在实施奖惩制度时，应确保员工合法权益。

7.2.5 权益保护

7.2.5.1 鼓励员工举报违反企业商业秘密管理规定的行为，并保证举报人的合法权益不受侵犯。

7.2.5.2 企业应设立专门的举报渠道，确保举报信息能够及时得到处理，并对举报人身份严格保密。

7.2.5.3　企业应设立相应的申诉渠道，保障员工对奖惩决定提出异议。

7.3　人员管理

7.3.1　入职管理

7.3.1.1　背景调查

7.3.1.1.1　对涉密重点岗位的拟入职人员进行全面的背景调查，包括但不限于以下内容：

a）　教育背景及经历；
b）　过往任职单位及工作内容；
c）　职务及专业资格；
d）　是否涉及知识产权纠纷等；
e）　是否曾签订过竞业限制协议等。

注：为确保调查结果的准确性和全面性，必要时可聘用第三方机构。

7.3.1.1.2　对于拟录用存在竞争性关系企业的人员，应进行身份、背景、专业资格等全面审查，重点关注其离职原因、离职时间、原单位保密协议内容等。

7.3.1.1.3　应提醒拟入职人员不应将原单位的商业秘密带入本企业进行使用或公开,并要求其签署保证书（见附录 A）。

7.3.1.2　保密协议

应与所有新入职人员签订保密协议（见附录 B），明确约定保密范围、保密期限、双方权利义务、违约责任等内容。

7.3.1.3　竞业限制协议

应与新入职的高级管理人员、高级技术人员及其他负有保密义务的人员签署竞业限制协议（见附录 C），并约定竞业限制的范围、地域、生效条件、期限、违约责任、经济补偿等内容。

7.3.2　在职管理

7.3.2.1　日常管理

7.3.2.1.1　根据涉密岗位及各部门的工作内容建立涉密人员清单，并定期更新。

7.3.2.1.2　根据商业秘密清单、接触商业秘密的情况等动态更新涉密岗位及涉密人员清单,完善制度，做好日常保密培训。

7.3.2.1.3　定期梳理高级管理人员、高级技术人员和其他知悉核心、重要商业秘密的人员，确定是否补签竞业限制协议。

7.3.2.2　行为规范

企业应确保工作人员遵守商业秘密保护制度，采取的措施包括但不限于：

a）　涉密信息及涉密载体应及时上报，有专人归档统一管理；
b）　使用涉密信息应履行登记手续，严格按照规定的途径和要求使用、流转；
c）　离开工作岗位前应及时下线工作账户，设置电脑锁屏等安全措施；
d）　不得登录未授权账户，不得超范围使用涉密文件资料、物品、数据；

e） 不得复制、发送涉密电子文档，不得将涉密电子文档存于未授权载体或网络空间；
f） 不得拍摄、摘抄涉密资料，不得拍摄、测绘、仿造涉密物品；
g） 不得进入非授权涉密区域，不得披露企业未公开的信息。

7.3.2.3 行为限制

7.3.2.3.1 对于中高层管理人员和涉密重要岗位人员，企业应对以下行为进行限制，具体包括：
a） 禁止兼职、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） 禁止与上述企业进行任何形式的商业交易；
c） 禁止与所在企业存在竞争关系的企业进行涉及商业秘密的交易。

7.3.2.3.2 对于涉密岗位的工作人员，企业应采取以下额外措施，具体包括：
a） 定期审核涉密岗位工作人员的访问权限，确保其只能够访问其工作必需的信息；
b） 对涉密岗位工作人员的工作电脑进行定期检查，确保没有异常操作记录；
c） 加强对涉密岗位工作人员的进出记录管理，确保其出入涉密区域的行为符合规定；
d） 定期对涉密岗位工作人员进行一对一的保密谈话，了解其对保密规定的理解和执行情况。

7.3.3 离职管理

7.3.3.1 离职谈话

涉密岗位员工离职前应与其谈话，形成谈话记录并由双方签字确认，谈话内容可包括但不限于：
a） 明确商业秘密范围；
b） 告知其应承担的保密义务；
c） 提示其不应有以下行为：
复制、带离、损毁、篡改、拍摄涉密资料、涉密物品；
查阅、拷贝、篡改、发送涉密电子信息；
删除、更改账户；
披露、使用或允许他人使用商业秘密等。
d） 违反规定应承担的相应法律责任。

7.3.3.2 离职检查

对离职员工进行离岗前检查，并形成书面报告，检查内容包括但不限于：
a） 工作电脑数据是否完整；
b） 工作账户是否有异常操作，如异常查询、下载、拷贝、修改、删除等；
c） 离职前一定期限内的涉密资料、涉密物品的查阅和使用情况等。

7.3.3.3 脱密

7.3.3.3.1 收回离职人员的相应工作权限，如回收或注销离职人员所有的域名、应用系统、网络系统、门禁系统账号或访问权限等。通知有关的供应商、客户、合作单位等相关方，做好业务对接。

7.3.3.3.2 应要求离职人员主动交接所有涉密载体和物品，包括但不限于：
a） 涉密资料、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、钥匙等。

7.3.3.3.3　根据离职人员所接触涉密信息的密级、重要程度及潜在风险等，明确脱密期限，并对处于脱密期内的离职人员进行保密提醒及监督检查。

7.3.3.4　竞业限制实施

应根据企业需要决定是否对离职人员启动或解除竞业限制,决定启动时应明确竞业限制费用的发放及竞业限制协议的履行情况，并应及时掌握离职人员在竞业限制期限内的任职情况。

7.3.4　外部人员管理

7.3.4.1　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。

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

7.3.4.3　对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，应做背景调查，并签署保密协议。

7.4　涉密载体管理

7.4.1　制作

7.4.1.1　定密与标识

7.4.1.1.1　在制作包含商业秘密信息的涉密载体时，应明确其密级并标记相应的保密标识。

7.4.1.1.2　应建立详细的记录档案，在发放时严格按照批准的范围执行，并做好发放记录。

7.4.1.2　采取的措施

7.4.1.2.1　制作过程应指定专人负责，并确保在完成后销毁所有无用的中间产物。

7.4.1.2.2　委托外部单位制作时，应事先签订保密协议或在合同条款中明确保密事项及违约责任。

7.4.1.2.3　制作过程中形成的草稿、校样、印版、底片和废品等，应及时在专人监督下销毁。

7.4.2　收发与传递

7.4.2.1　接收程序

涉密载体的接收和发送应指定专人操作，并执行清点和签收确认等程序。

7.4.2.2　禁止方式

禁止通过普通传真机、公用电子邮件、手机短信、聊天软件、普通邮政等方式传递涉密信息。

7.4.2.3　内部传递

企业内部不同部门间的传递应使用专业办公软件或专人密封报送。

7.4.3　使用

7.4.3.1　标识与管理

涉密信息载体应清晰标注其密级、保护期限等标识，并实行登记管理、归档存放。

7.4.3.2　权限控制

7.4.3.2.1　按权限使用，查阅、借阅、续借应履行登记手续。

7.4.3.2.2　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。

7.4.3.3　信息发布

发布任何形式的公开信息（如新闻、论文、专利申请等）之前，由商业秘密保护部门对信息进行审核。

7.4.4　复制

7.4.4.1　涉密载体的复制应由所在部门负责人审核，并经商业秘密保护部门批准。

7.4.4.2　复制品应视为原件管理，并做好登记。

7.4.4.3　对于核心商业秘密，严禁任何形式的复制行为。

7.4.5　保管

7.4.5.1　保存环境

涉密载体的保管应选择专门的保密区域或具备安全保障条件的场所、部位、设备。

7.4.5.2　交接手续

7.4.5.2.1　管理人员离职前，应办理交接手续。

7.4.5.2.2　被撤销、合并的单位，应将秘密载体移交承担原职能的单位或保密部门，并履行必要的交接程序。

7.4.6　销毁

7.4.6.1　销毁审批

销毁涉密载体前，应由商业秘密管理保护部门审核，经企业最高管理层批准。

7.4.6.2　销毁记录

7.4.6.2.1　销毁前应履行登记手续，销毁工作应在指定的地点按照规定的方法进行，并在专人监督下销毁。

7.4.6.2.2　纸质涉密文件应使用碎纸机处理，未经切碎的文件严禁作收购处理。

7.4.7　涉密电子信息管理

7.4.7.1　储存要求

7.4.7.1.1　涉密数据应存储于企业授权的存储设备和应用系统或受控的云存储空间。

7.4.7.1.2　核心、重要商业秘密等级的数据应采用加密方式存储，并定期备份、妥善保存。

7.4.7.2　权限管理

7.4.7.2.1　对设备、数据库及各类应用系统及其账户实行权限管理，依照岗位职责或特定工作事项按“最小必要”原则设定权限。

7.4.7.2.2　权限到期、人员转岗、项目或事项变更时，应重新评估和调整权限。

7.4.7.2.3　人员离职时应回收相应权限。

7.4.7.3　账户与密码

7.4.7.3.1　各类设备、数据库和应用系统应设账户和密码，不应使用默认密码或保存密码自动登录功能。

7.4.7.3.2　根据企业的业务类型采取适当的账户、密码管理方式，如限制使用简单密码、必要时不定期更改密码、输错密码一定次数锁定账户等。

7.4.7.3.3　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。

7.4.7.4　流转管理

7.4.7.4.1　收发涉密数据应使用唯一出入口，对涉密数据流入流出进行审批。

7.4.7.4.2　必要时，使内部局域网与互联网隔离，涉密数据网络传递应通过内部局域网或加密互联网通道完成。

7.4.7.4.3　通过邮件发送涉密数据时，应加密和签名，可限定文档打开次数、打开时限和编辑权限等。

7.4.7.4.4　对外发送涉密数据应经过审批，并采取加密措施，数据发送与密钥发送不宜采用同一通道。

7.4.7.4.5　应与客户、合作单位等涉密数据接收相关方或个人签订保密协议。

7.4.8　物理涉密载体管理

7.4.8.1　妥善保管

7.4.8.1.1　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。

7.4.8.1.2　涉密载体存放地点宜设为涉密重点区域，采取物理隔离的方式进行保护。

7.4.8.2　禁止行为

未经商业秘密保护部门、法定代表人或其授权人审批，不得拍摄、测绘或仿造。

7.4.8.3　登记管理

7.4.8.3.1　部门内专（兼）职保密员负责登记造册，并按照权限级别使用、领取涉密载体时应履行登记手续。

7.4.8.3.2　跨区域转移涉密载体应履行审批手续，必要时采取防护措施。

7.4.8.4　报废销毁

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

7.5　涉密区域管理

7.5.1　涉密区域识别

企业应明确界定涉密区域，并在入口处设置显著的涉密区域标志和警示标识。涉密区域包括但不限于：

a）研发设计部门、实验场所、重要生产工作场所；

b）控制中心、数据中心机房；

c）涉密文档、涉密载体存放地点；

d） 重要样品、模具、专用工具、关键零部件等的存放区；

e） 关键原材料、重要半成品等物资的储存区等。

7.5.2 涉密区域保护

7.5.2.1 涉密区域与非涉密区域之间应设置物理隔离屏障，如墙壁、门禁等，必要时可增设网络隔离措施。

7.5.2.2 涉密区域的出入口应设置门禁系统，并明确标识；人员进入需通过授权验证，宜采用指纹、面部识别等生物识别技术手段进行身份验证，并实行进出登记手续。

7.5.2.3 涉密区域出入口及内部应安装视频监控系统,宜使用高清摄像头,实时监控并识别异常行为，并安装报警装置，防止非法入侵。

7.5.2.4 涉密区域内可设置宣传画报、标语等，强化商业秘密保护意识。

7.5.2.5 涉密资料和物品在涉密区域间的转移需经过审批，并进行记录。

7.5.2.6 限制在涉密区域内使用带有录音、录像、拍照、信息存储功能的设备，必要时实施网络隔离。

7.5.3 涉密区域网络管理

7.5.3.1 涉密网络区域禁止使用有线或无线形式接入外网，应与其他内部网络物理隔离。

7.5.3.2 涉密网络区域与其他内部网络采取差异化的管理措施。

7.5.3.3 访问涉密区域网络的设备需符合终端准入要求。

7.5.3.4 通过虚拟专用网络（VPN）等方式远程访问涉密区域网络时，需满足终端准入和身份验证条件。

7.5.3.5 涉密区域应配备独立的网络基础设施，如服务器、防火墙等。

7.5.4 涉密区域出入管理

7.5.4.1 涉密区域实行进出登记，限制外来人员进入；确需进入的应经过审批，并全程监督。

7.5.4.2 应在外来人员进入涉密区域前进行保密事项提醒，要求其佩戴临时访问证件，并履行进出登记手续。

7.5.4.3 应设置临时储物柜供来访人员存放个人物品。

7.5.4.4 外来人员进入涉密区域时，应由接待部门安排专人陪同，并限制使用录音、录像、拍照等设备。

7.5.5 涉密区域设备管理

7.5.5.1 涉密计算机应配备防止偷窥和拍照的措施。

7.5.5.2 涉密设备如研发图文档系统、资料管理系统等应合理配置权限。

7.5.5.3 合理分配不同层级账户的功能和审批权限，确保权限合理使用。

7.5.5.4 各类设备、数据库和应用系统应设置账户密码，避免使用默认密码或自动登录功能，并定期更换密码。

7.6 商务活动管理

7.6.1 会议管理

7.6.1.1 安排涉密会议时，应明确会议的主题、时间、地点、参会人员，并提前进行保密培训。

7.6.1.2 涉密会议应在涉密区域内召开，并使用专用或临时的保密会议室。

7.6.1.3 参会人员应具备接触所涉商业秘密的权限或经审批，并事先告知保密要求或签署保密承诺。

7.6.1.4 限制使用手机、便携式设备或具有录音、录像、拍照、信息存储等功能的设备。

7.6.1.5 会议记录应进行保密处理，记录人应具备相应的权限，并对记录进行归档和管理。

7.6.1.6 会议结束后，应清理现场，确保无遗留涉密资料，并对会议内容进行保密审查。

7.6.2 合作管理

7.6.2.1 选择供应商、客户等合作伙伴时应评估其商业信誉和保密能力,并签订商务合作保密协议(见附录 D）。

7.6.2.2 与合作伙伴签订的协议中应包含保密条款，明确双方的保密义务及违约责任。

7.6.2.3 提供技术支持或共享商业秘密时，应明确保密范围和期限，并采取必要的技术保护措施。

7.6.2.4 与合作伙伴的数据交换应通过加密或其他安全措施进行，并限制访问权限。

7.6.2.5 专家、顾问等短期接触涉密信息的，应使用保密计算机并对信息进行加密。

7.6.2.6 涉密项目需长期合作的，应与参与项目的合作伙伴员工签订个人保密协议。

7.6.3 参观管理

7.6.3.1 为来访人员设定专门的参观路线，以避开涉密区域。

7.6.3.2 来访人员进入涉密区域应由专人全程陪同，并限制其使用具有录音、录像、拍照、信息存储等功能的设备。

7.6.3.3 来访人员应佩戴临时证件，并履行进出登记手续。

7.6.3.4 在参观过程中，应向来访人员告知保密要求，并要求其签署保密承诺。

7.6.3.5 参观过程中应进行视频监控，确保无异常行为。

8 商业秘密维权

8.1 应急处理

8.1.1 应急预案制定

8.1.1.1 企业应制定详细的商业秘密泄露应急预案，明确应急处理流程，包括应急响应级别、应急指挥机构、应急响应程序、应急处置措施、应急资源保障等内容。

8.1.1.2 根据实际演练和经验反馈，应定期修订和完善应急预案，确保其有效性。

8.1.2 应急演练

应定期组织应急预案演练，提高员工的应急反应能力。应通过模拟不同类型的泄露情景，检验应急预案的有效性。演练结束后，应总结演练情况，改进不足之处。

8.1.3 应急响应

发现商业秘密可能被泄露或侵权，应立即启动应急预案，及时采取措施，如立即停止相关人员的访问权限、封存相关设备和文件等，控制事态发展，防止损失扩大。

8.2 证据搜集

8.2.1 证据固定

发现商业秘密被泄露或侵权，应立即收集相关证据，包括但不限于：

a） 企业拥有商业秘密的相关证据，如商业秘密的具体内容、载体、不为公众所知悉的证明、对商业秘密所采取的保密措施等；

b） 商业秘密被侵权的证据，如侵权行为的具体表现、侵权人的相关信息、侵权行为造成的损失等；

c） 可能与泄密信息有关的人员的信息，如在职员工、离职员工、退休员工的工作经历、工作内容、接触到的涉密信息、接受保密培训的记录、与企业签订的商业秘密保护合同等；

d） 其他相关证据，如第三方的证言、相关的物证、书证等。

8.2.2 证据保存

收集的证据应妥善保存，确保其真实性、完整性和有效性。对收集的证据进行分类、整理，便于后续使用。重要证据应进行备份，以防丢失或损坏；必要时，可向商业秘密保护服务机构或专业机构寻求帮助，进行证据保全公证。

8.2.3 证据展示

在维权过程中，准备好展示证据所需的材料和技术手段。根据具体情况选择合适的展示方式，如书面材料、电子文档、视频资料等。

8.3 技术支持

8.3.1 技术保护措施

使用加密技术保护商业秘密信息，确保其传输和存储的安全性。对涉密信息系统采取严格的访问控制措施，确保只有授权人员可以访问。定期进行数据备份，防止数据丢失或损坏。

8.3.2 技术监控

安装视频监控系统和报警装置，确保任何非法闯入行为都能立即被监测到并触发警报。安装高清摄像头，实时监控并识别异常行为。对网络流量进行监控，防止非法数据传输。

8.3.3 技术辅助

使用专业的取证工具，确保收集的证据真实可靠。利用数据分析技术，分析可能存在的安全隐患和漏洞。组建专业的技术支持团队，负责技术支持工作。

8.4 维权途径

8.4.1 行政途径

向有管辖权的商业秘密行政管理部门举报，要求查处商业秘密侵权行为。配合行政部门进行调查处理，确保侵权行为得到制止。

8.4.2 民事诉讼

向侵权行为发生地或侵权人所在地等有管辖权的人民法院提起民事诉讼，请求赔偿损失。向有管辖权的法院申请诉前禁令，阻止侵权行为继续发生。

8.4.3 刑事控告

符合刑事案件立案条件的，向犯罪行为发生地的公安机关报案，要求追究侵权人的刑事责任。配合公安机关进行调查取证，确保案件顺利进行。

8.4.4 劳动仲裁

违反竞业限制协议等属于劳动仲裁受案范围的，应先向企业所在地等有管辖权的劳动仲裁委员会申请劳动仲裁。准备好相关证据和材料，确保仲裁顺利进行。

8.4.5 商事仲裁

第三方企业违反协议约定的保密义务且约定商事仲裁管辖条款的，应向约定的仲裁委员会申请仲裁。准备好相关证据和材料，确保仲裁顺利进行。

8.4.6 协调解决

在侵权行为初期，可以尝试通过协商解决争议，达成和解协议。通过调解机构进行调解，争取达成调解协议。

附　录　A
（资料性）
不侵犯商业秘密保证书（参考文本）

保证人：

身份证号：

鉴于保证人曾任职于其他单位，并可能接触、知悉或掌握与原单位相关的商业秘密，为保证人现就职单位（以下简称“本单位”）的合法权益及商业秘密安全，保证人特此向本单位作出如下承诺：

一、声明与承诺

1.保证人声明，在离职原单位时，严格遵循相关法律法规及原单位的规定流程，对所有在原单位工作期间接触、知悉或掌握的商业秘密，包括但不限于技术信息（如设计图纸、工艺流程、技术配方等）、经营信息（如采购渠道、销售策略、财务数据等）、客户信息（如客户名单、客户需求偏好、交易记录等）以及其他具有商业价值且不为公众所知悉的信息，进行了全面清查与处理。对于能归还的商业秘密载体，如纸质文件、电子存储设备等，已如数归还给原单位，并取得原单位的书面接收确认；对于无法归还或已无必要归还的商业秘密信息，已采用不可恢复的方式进行销毁，销毁过程有详细记录并存档备查，确保未以任何形式保留原单位的商业秘密。

2.保证人承诺，在本单位任职期间，不使用、不泄露、不传播、不利用任何原单位的商业秘密，确保本单位的商业秘密安全。不将原单位的商业秘密以任何方式带入单位，包括但不限于电子文件、纸质文件、口头信息以及其他任何形式的信息载体；不利用原单位的商业秘密进行任何形式的研发、生产、经营活动，或以任何方式促使单位使用原单位的商业秘密。将严格遵守本单位的保密制度，避免在非工作场所（如公共场所、社交聚会等）谈论涉及本单位或原单位商业秘密的敏感话题，防止因无意疏忽而导致商业秘密泄露。

二、保密义务

1.保证人对在本单位任职期间所接触、知悉或掌握的商业秘密承担严格的保密义务。本单位的商业秘密是指本单位在生产经营过程中形成的，具有商业价值且不为公众所知悉，并经本单位采取合理保密措施予以保护的各类信息，包括但不限于技术方案、产品设计、制造方法、工艺流程、销售渠道、客户名单、财务数据、价格体系、商业计划、市场调研分析报告、计算机软件源代码及算法、数据库结构以及其他与本单位业务相关的信息及资料。未经本单位书面同意，保证人不得向任何第三方披露、使用、允许他人使用或为自己或他人谋取利益而利用上述商业秘密。

2.保证人离职后，仍将继续承担上述保密义务，直至相关商业秘密已为公众所知悉或因技术进步、市场变化等客观原因失去保密价值。在保密义务存续期间，保证人应妥善保管与商业秘密相关的任何信息，不得擅自披露或使用，即使在非工作场景下亦应保持高度警惕，防止因个人行为导致商业秘密泄露。

三、法律责任

1.保证人违反本保证书的任何条款，愿意承担相应的法律责任。保证人同意向本单位支付违约金，违约金金额为人民币元（或根据双方约定的计算方式确定，如按照保证人在本单位的年薪倍数计算等）。

2.保证人同意，如有第三方因保证人的行为而对单位提起诉讼或采取其他法律措施，保证人将全力配合单位进行抗辩，并承担因此产生的所有费用，包括但不限于聘请律师的费用、出庭应诉的费用、提供证据的费用以及与案件相关的其他合理费用。保证人应在接到本单位通知后的个工作日内，向本单位提供其所知悉的与案件相关的所有信息和资料，并积极协助本单位制定应对策略。

四、其他条款

1.本保证书自保证人签署之日起生效，直至保证人离职后(填写具体时长)内仍具有法律效力。在保证书有效期内，若相关法律法规或本单位的保密政策发生变化，保证人应遵守新的规定，并根据本单位的要求对本保证书进行相应的修订或补充。

2.本保证书一式两份，单位和保证人各执一份，具有同等法律效力。

保证人（签字）：

年月日

注：本保证书未尽事宜，双方可另行协商补充。在签署本保证书前，本人已充分阅读并理解本保证书的所有内容，自愿承担相应的法律责任。本保证书旨在保护单位的商业秘密和知识产权，适用于所有与单位商业秘密相关的保证事项。

附　录　B

（资料性）

员工保密协议（参考文本）

甲方（用人单位）：

乙方（劳 动 者）：

居民身份证号码：

因乙方现正在为甲方提供服务和履行职务，已经（或将要）知悉甲方的商业秘密。为了明确乙方的保密义务，有效保护甲方的商业秘密，防止该商业秘密被公开披露或以任何形式泄漏，根据《中华人民共和国合同法》《中华人民共和国劳动法》《中华人民共和国反不正当竞争法》及国务院有关部委的相关规定，甲、乙双方本着平等、自愿、公平和诚实信用的原则签订本保密协议。订立下列条款并共同遵守。本合同之签订可认为甲方已对甲方的商业秘密采取了合理的保密措施。

一、商业秘密的范围

本合同所称“商业秘密”包括但不限于：技术信息、经营信息、专有技术、客户信息、内部秘密以及其他商业信息等。乙方对此商业秘密承担保密义务。

1.技术信息包括但不限于：特定产品或项目的技术方案（如产品的独特设计思路、工艺流程的关键环节、技术创新点等）、工程设计、电路设计、技术指标、计算机软件（包括源代码、算法、程序架构等）、数据库（数据结构、数据存储逻辑、数据更新机制等）、研究开发记录（研发过程中的实验数据、技术难点突破记录、技术改进过程等）、技术报告、检测报告、实验数据、试验结果、图纸（包括产品设计图、工程施工图、工艺流程图等）、操作手册、技术文档、相关的函电等技术方面的秘密。

2.经营信息包括但不限于：客户名单（包括现有客户、潜在客户，涵盖客户的姓名、性别、身份证信息、手机号码、家庭住址、工作单位、购票相关信息、乘车相关信息、个人需求、消费偏好、购买频率、特殊要求等信息以及客户与甲方的交易历史、交易金额、合作意向等）、营销计划（市场推广策略、促销活动方案、品牌建设规划等）、采购资料（供应商信息、采购价格、采购数量、采购周期等）、定价政策、投资计划或者方案、发展规划、财务资料（财务报表、财务预算、成本核算数据等）、货源情报、业务渠道、工作流程（内部业务操作规范、审批流程等）、谈判底价、招投标标书或者底标、经营诀窍、企业内部网上的信息、程序文件、情报文件、公司档案、法律事务信息、人力资源信息（员工薪酬体系、绩效考核方案、人才储备计划等）等经营方面的秘密，以及专利申请文件等与知识产权相关的保密事项。

3.专有技术：是指甲方拥有的有关生产的信息、资料、流程、经验、方法或其组合，并且未在任何地方公开过其完整形式的、未作为产权来保护的其他技术。

4.客户信息包括但不限于：客户的姓名、性别、身份证信息、手机号码、家庭住址、工作单位、购票相关信息、乘车相关信息、个人需求、录音等信息、文件、资料、图表、报告、信件、传真、磁带、磁盘以及其他任何形式的载体所载信息，无论这些信息有无商业价值。

5.内部秘密包括但不限于：企业内部的重大决策、内部人事任免信息、内部财务审计报告、未公开的会议内容、内部培训资料、内部沟通邮件、内部通知、企业内部网络架构、账号密码、门禁密码、安全防护措施等仅在企业内部流通且具有保密性的信息。

6.其他商业信息包括但不限于：甲方在经营过程中获得的其他未公开且具有商业价值的信息，如

行业动态信息、政策法规解读信息、政府项目申报信息等，以及根据其性质或甲方采取保密措施而应被认定为商业秘密的信息。

7.同时，在甲方生产或者经营中，某一信息的泄露可能造成下述后果之一的，该信息也属于甲方商业秘密：

（1）影响甲方生产、营销、稳定、安全或者发展的；

（2）影响甲方技术进步的；

（3）使甲方利益受到损害，或者使甲方在商业竞争中处于被动或不利地位的；

（4）影响甲方对外交流或商业谈判顺利进行的；

（5）影响甲方对外承担保密义务的。

8.甲方在记录某一技术信息或者经营信息的载体上注明“保密”或“内部资料”等字样，或者载明保密等级的，该信息属于商业秘密。

9.本协议所称商业秘密，包括属于甲方或者虽属于第三方但甲方承诺有保密义务的商业秘密。

10.关于反向工程，除非甲方明确许可，乙方承诺不通过技术手段对甲方产品进行拆卸、测绘、分析等方式而获得该产品的有关技术信息，否则视为侵犯甲方商业秘密。

二、商业秘密的载体

1.乙方持有或保管的一切记录有甲方商业秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器、电子邮件以及其它任何形式的载体均归甲方所有，无论这些信息是否具有商业价值。

2.未经甲方许可或者非因履行甲方职务所需，乙方在任职期间或者离职后，不得擅自对前述载体进行复制，也不得将载体或者复制件遗弃、怠于保管或者交给他人。若乙方因工作需要对载体进行复制，应事先获得甲方书面批准，并记录复制的用途、份数、使用人员等信息，复制件应与原件同等管理。

3.乙方应当于离职时，或者于甲方提出请求时，返还前述载体和复制件给甲方。乙方应确保返还的载体和复制件完整、无损坏，若有缺失或损坏应承担相应责任。

三、职务成果

1.与乙方职务相关的智力成果，包括但不限于因履行职务、利用工作时间，或者利用甲方的物质技术条件等完成或者产生的任何发明创造、发现、研究、设计、改进、创新成果、作品、计算机软件、商业秘密等，以及由此获得的知识产权，均属于甲方所有；甲方可自由利用进行生产、经营或者转让给第三人。

2.乙方有义务为职务成果保守秘密，并应当积极提供一切必要的信息和采取一切必要的行动（包括但不限于申请、注册、登记等），协助甲方取得和行使有关的知识产权或者所有权。若因乙方原因导致在协助甲方取得知识产权或所有权过程中出现延误、失败或产生纠纷，乙方应承担相应责任，包括但不限于赔偿甲方因此遭受的损失（如因延误导致的市场机会丧失、因纠纷产生的法律费用等）。

四、保密制度

1.乙方应当遵守国家与保密相关的法律、法规。

2.乙方应当严格遵守甲方的任何成文或者不成文的保密制度，并履行与其工作岗位相应的保密职责。

3.甲方的保密制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚信、负责的态度，采取必要和合理的措施，保守其知悉或者持有的商业秘密。

4.解密期：乙方在任职期间如接触到具有重大价值的商业秘密，甲方有权在劳动合同期限届满前一年时间内将乙方调整到其他部门工作，并按新岗位标准调整乙方薪酬。新岗位工作内容应与原接触商业秘密的关联程度较低，避免乙方继续接触或利用原商业秘密。新岗位薪酬调整应依据甲方内部薪酬调整政策，综合考虑乙方的工作经验、技能水平等因素确定合理幅度范围。此规定无需经济补偿，

亦不影响乙方继续履行本合同确定的保密和竞业限制义务。

5.对外合作与信息披露：面对外部合作方、第三方机构或公共事务处理时，乙方应遵循甲方规定的保密规范和信息披露审批流程。未经甲方书面批准，乙方不得向任何外部方透露甲方商业秘密，若因业务需要必须披露，应提前向甲方提交披露申请，说明披露的目的、对象、内容等，经甲方审核批准后方可进行披露，并在披露过程中严格控制披露范围和程度。

五、保密责任

1.乙方不得以盗窃、利诱、胁迫或者其他不正当手段获取甲方商业秘密。

2.未经甲方书面同意，乙方不得泄露、告知、公布、发表、出版、传播、传授、转让或者以遗弃或者怠于保管等其它任何方式使任何第三方（包括无权知悉该项商业秘密的甲方其他职员）知悉甲方商业秘密，也不得在履行职务之外使用这些商业秘密。乙方在使用甲方商业秘密时，应遵循甲方规定的权限限制，记录使用的时间、用途、涉及的商业秘密内容等信息，便于追溯和审计。

3.乙方在任职期间，以及无论何种原因离职（含甲方或者乙方解除或者终止劳动合同）后，均应对其接触、知悉的甲方商业秘密，承担保密义务，直到甲方宣布解密或者有关秘密信息实际已经公开为止（但因乙方非正当公开的除外）。

4.乙方承诺：在为甲方履行职务时，不得擅自使用任何属于他人的商业秘密，也不得擅自实施可能侵犯他人知识产权的行为。否则，导致甲方遭受第三人侵权指控，甲方因此而承担侵权赔偿责任的，有权向乙方追偿；同时乙方应当承担甲方为应诉而支付的一切费用。

5.乙方认可所收取的劳动报酬已经考虑其任职期间或者离职后所承担的保密义务，并认可承担保密义务是其履行劳动合同的附随和法定义务，甲方无需另行支付保密费。

6.乙方在发现他人有侵犯甲方商业秘密行为时，有义务及时向甲方报告。若因乙方报告使得甲方成功制止侵权行为或挽回损失，甲方可给予乙方一定的奖励（如奖金、荣誉表彰等）。

7.乙方在任职期间或者离职后，均不得引诱甲方其他员工离职，否则视为侵犯甲方商业秘密。

六、兼职限制

未经甲方书面同意，乙方任职期间不得到其他用人单位工作或者兼职。

七、竞业限制双方选择（1.订立；2.暂不订立）

1.在乙方离职（劳动合同被解除或者终止）后 24 个月内，乙方不得到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或兼职，也不得自己开业生产或者经营同类产品、从事同类业务。

2.乙方按照甲方规定遵守竞业限制约定的，在竞业限制期限内，甲方每月支付乙方补偿费元。

3.甲方有权根据乙方掌握商业秘密的实际情况，在乙方离职时、或者在竞业限制期限内以书面形式通知乙方终止竞业限制约定（终止后不再支付补偿费）。

八、违约责任

1.乙方违反本合同第四条（保密制度）、第五条（保密责任）、第六条（兼职限制）规定的，属于“严重违反甲方规章制度”的行为，甲方有权单方与乙方即时解除劳动合同，并且不向乙方支付任何经济补偿。

2.乙方违反本合同约定，或者侵犯甲方商业秘密的，应当对造成甲方的损失承担赔偿责任。甲方的损失，包括但不限于实际损失、间接损失（含预期利益）以及甲方因调查或制止乙方违约或者侵权行为而支付的合理费用（例如差旅费、鉴定费、诉讼费、仲裁费、律师费）等。对于甲方损失的评估，可由双方共同认可的专业第三方评估机构进行评估，或按照行业通行的评估标准和方法确定。

3.乙方违反竞业限制约定的，除返还已经收取的竞业限制补偿外，应向甲方支付违约金元；违约金不足以赔偿甲方损失的，按实际损失赔偿。乙方的违约行为还将对其个人职业声誉、行业信誉产生负面影响，甲方有权将乙方的违约情况通报给相关行业协会、企业合作方等，以警示其他企业防范类似风险。

4.乙方承担违约赔偿责任并不免除其继续按照本合同承担保密义务或者竞业限制义务。

九、争议解决

1.因履行本合同发生争议，由双方协商解决；协商不成的，双方可选择以下争议解决方式：

（1）向甲方所在地人民法院提起诉讼解决；

（2）向仲裁委员会申请仲裁，按照该仲裁机构的仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

2.前述约定不影响甲方请求知识产权管理部门对侵权行为进行处理。

十、其它事项

1.乙方确认已经充分了解甲方有关保密的全部程序文件和管理规定，并自愿遵守执行。

2.本合同所称“离职”，以任何一方明确表明解除或者终止劳动关系的时间为准。乙方拒绝领取工资或者停止履行职务的行为视为提出离职。

3.本合同第六条、第七条所称“工作”或“兼职”，均包括但不限于担任股东、合伙人、董事、监事、经理、职员、代理人、顾问等，还包括提供其他形式的服务（含有偿或无偿）。

4.本合同第七条所称“产品”或者“业务”，包括甲方营业执照列明范围以及甲方实际或计划经营的产品或者业务。

5.本合同是双方签订劳动合同的组成部分，本合同内容如与劳动合同或者甲方规章制度抵触的，以本合同为准。

6.本合同的变更必须采用书面形式。

7.甲、乙双方在本合同履行过程中相互发出或者提供的所有通知、文件等，均可以当面交付或以《劳动合同书》列明的通讯地址履行送达义务；一方如果迁址或变更电话，应当及时书面通知对方；按前述地址的寄送无论对方拒收，或因地址不详等原因被退回的，均视为合法有效的送达。

8.本合同正本一式二份，甲、乙双方各执一份，均具同等法律效力。合同自双方签字、盖章之日起生效。

甲方：　　乙方（签字捺手印）：

法定代表人：　　住址：联系电话：

年月日　　年月日

附 录 C

（资料性）

竞业限制协议（参考文本）

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：

鉴于乙方在甲方履行职务，已经（或将要）知悉甲方的商业秘密，或者对甲方的竞争优势具有重要影响。为保护双方合法权益，甲、乙双方特根据《中华人民共和国反不正当竞争法》《中华人民共和国公司法》《中华人民共和国劳动合同法》及国家、地方有关规定，本着平等自愿、协商一致、诚实守信的原则，经充分协商一致后，就竞业限制事宜,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）签署本协议以共同执行：

一、竞业限制范围

未经甲方书面同意，乙方在双方劳动合同关系终止之后_____月内不得从事下列竞业限制事项：

1.不得在离职后在与甲方具有竞争关系的企业、事业单位及社会团体内担任任何职务，包括股东、合伙人、董事、监事、经理、职员、代理人、顾问等，不得受聘于上述单位或者岗位。与甲方有竞争关系的企业主要有：等，但不限于上述单位。

2.不得自己经营或与他人合作经营从事与甲方具有竞争关系的业务。

3.乙方承诺，在离职之前或者离职之后竞业限制期内，不得抢夺乙方客户，不得利用甲方资源获取利益、盗用课件、流程、咨询协议书、咨询流程、商业机密；不得以许诺高薪、职务、高福利等手段诱使甲方在职员工跳槽，损害甲方的合法权益。

4.竞业限制的区域范围为：第类。

（1）全国范围内。

（2）甲方注册地所在城市：。

（3）双方约定的省市：。

二、竞业补偿标准

由于乙方接受甲方竞业要求，会对乙方造成一定的影响和相应的经济损失，因此甲方给予乙方一定的竞业补偿金，该补偿金标准按照不低于乙方离职前十二个月从甲方获得的报酬总额的%计算，补偿金总额为元。

三、竞业补偿金的支付

1.竞业补偿金的支付采取按月支付的方式，在每月 15-20 日期间支付。

2.竞业补偿金领取过程中，乙方必须定期提供就业情况说明。

每季度末最后一个月 20 日前，乙方需通过 EMS 提供一份就业情况说明，写明是待业、自营或合营何种类型的单位、在单位就职的要求提供在职证明，在职证明要求写明具体的企业名称、企业注册地址、

单位联系电话、就职部门和职务。

3.支付方式为向乙方银行卡转账支付，乙方银行卡持有人姓名，银行卡属于银行，卡号为。乙方承诺提供的银行卡在竞业限制期间保持正常使用状态，如中途换卡、销户、挂失等原因未及时书面通知甲方的，视为乙方过失，甲方不承担延迟支付补偿金责任或其他责任，补偿金由乙方本人来甲方领取或重新提供卡号打卡。

四、违约责任

1.乙方如果违反本协议约定，从事了竞业事项，应当向甲方支付违约金，违约金标准按照离职前岗位确定，乙方违规不及时支付时，每增加一日，加收%的滞纳金。同时符合以下几类的按照违约金标准高的支付：高管人员（总经理、副总经理、总监、副总监、其他高级管理岗位）违约金标准为元；专业、技术类人员（如：讲师、咨询师等公司关键岗位人员）违约金标准为元，信息类技术人员违约金标准为元。

该违约金的支付不影响甲方要求乙方赔偿因为从事竞业事项或其他行为给甲方造成的其他损失，也不影响甲方追究乙方的其他法律责任。

2.乙方未定期提供就业情况说明的，按照每延迟一次支付违约金_____元，连续三个月不提供就业情况说明的暂停竞业补偿金支付，竞业限制继续有效，提供就业情况说明后继续发放补偿金。

3、甲方因调查和处理乙方的违约行为而支付的合理费用（包括但不限于律师费、调查费、鉴定费、交通费、文印费、诉讼费等），应当包含在损害赔偿金额之内。

五、其他条款

1.签订本协议即说明乙方自愿遵守竞业限制义务，本协议不因经济补偿金未支付或未提供就业情况说明而终止，本协议自生效之日起除书面协商一致解除外，持续有效。

2.本协议未尽事宜经甲、乙双方友好协商解决。协商不成的，当事人向甲方企业注册地申请劳动仲裁、提起诉讼。

3.本协议一式两份，甲乙双方各执一份，签字或盖章后生效。

4.甲方已经按照乙方要求对本协议条款予以充分解释和说明，乙方确认其已清楚本协议每一条款的准确含义，并自愿签署及履行本协议。

（请员工本人手抄）：

甲　　方：（盖章）　　乙　　方：

法定代表人/授权代表：

日　　期：　　日　　期：

附 录 D
（资料性）
商务合作保密协议（参考文本）

甲　　方：
法定代表人：统一社会信用代码：
电　　话：传　　真：
地　　址：
联系人、电话及邮箱：

乙　　方：
法定代表人：统一社会信用代码：
电　　话：传　　真：
地　　址：
联系人、电话及邮箱：

甲乙双方正在就事项进行商务合作，双方在谈判或合作期间，均因合作需要可能接触或掌握对方有价值的保密信息（包括但不限于口头、书面或其他任何形式），双方本着平等自愿、协商一致、诚实守信的原则，为保护双方商业秘密事宜，于年月日（本协议生效日），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：

一、术语定义

本协议所称保密信息，系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等商业信息。

二、保密信息的范围

经双方确认，双方在谈判或合作履约期间，因合作需要可能接触或掌握对方有价值的保密信息，包括但不限于以下内容：

（1）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技术信息；

（2）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、数据等经营信息。其中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）其他符合商业秘密构成要件的商业信息。

注：此条仅供参考。实际使用时，企业可根据自身实际情况进行商业秘密范围的明确细化。

三、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.能证明获得相关信息时已经熟知的资料或信息。

3.由第三方合法提供给乙方的资料或信息。

4.未使用对方的技术资料，在日常业务中独立学习或研究获得的知识、信息或资料。

四、双方权利义务

1.未经一方书面同意，另一方（包括各自代表、员工）不得向第三方（包括新闻媒体或其从业人员）公开和披露任何保密信息，或以其他方式使用保密信息。

2.如谈判、合作项目不再继续进行，或相关合同解除、终止，一方有权在任何时候向另一方提出返还、销毁保密信息的书面要求，另一方应按要求在个工作日内向对方返还、销毁其占有的或控制的全部保密信息，包括但不限于保密信息的全部文件和其它材料。销毁方式应确保信息无法恢复，如采用粉碎纸质文件、删除电子数据并进行数据覆盖等方式，并保证不留有任何复制版本。

3.甲乙双方应以不低于其对己方拥有的类似资料的保密程度来对待对方向其披露的保密信息，但在任何情况下，对保密信息的保护都不能低于合理程度。

4.一方发现另一方有违反本协议的迹象时，有权书面通知违约方停止违约行为并要求采取补救措施，违约方应在接到通知之日起个工作日内予以回应和处理。

五、保密义务期限

甲乙双方互为保密信息的提供方和接受方，负有保密义务。本协议的保密期限，为本协议签订之日起至双方终止谈判或合作后年止。

六、知识产权

1.任何一方向另一方或其代表披露保密信息，并不代表同意另一方任意使用其保密信息、商标、专利、技术秘密及其它知识产权。

2.在合作过程中，若涉及基于保密信息产生的知识产权开发或合作成果，其归属及使用应依据双方另行签订的知识产权协议约定执行；若无相关约定，则依据法律法规确定归属，但任何一方使用相关成果均不得侵犯对方的保密信息权益。

七、保密信息的保存和使用

1.任何一方均有权在双方合作期间保存必要的保密信息，以履行约定义务。

2.在保密期限内，任何一方在应对合作项目的索赔、诉讼、及刑事控告等相关事宜时，有权合理使用保密信息。

3.如任何政府部门要求一方披露保密信息，应及时给予另一方书面通知，足以使另一方能够寻求保护令或其他适当的救济。如另一方没有获得保护或救济，或丧失取得保护或救济的权利，一方应仅在法律要求的范围内向政府部门披露相关保密信息，并且应尽合理义务根据另一方的要求对保密信息进行任何修改，并为披露的任何保密信息取得保密待遇。

八、违约责任

1.任何一方如违反本协议下的保密义务，应承担违约责任。双方约定，本协议项下之违约金（以下简称“违约金”），其违约金数额相当于双方拟达成或已达成合作金额的%。如本条款约定的上述违约金不足以弥补因违反保密义务而给受害方造成的损失,受害方有权进一步向侵权方主张损失赔偿。

2.在双方谈判或合作期间内,无论上述违约金给付与否，受害方均有权立即终止谈判或解除与违约方的合同、合作关系，因终止谈判或解除合同、合作所造成的缔约过失赔偿责任、合同赔偿损失由违约方自行承担。

3.损害赔偿的范围包括但不限于以下费用：

（1）受害方为处理此次纠纷支付的费用，包括但不限于律师费、诉讼费、差旅费、材料费、调查费、评估费、鉴定费等；

（2）受害方因此而遭受商业利益的损失，包括但不限于可得利益的损失、技术开发转让费用的损失等。

4.在保密期间内，任何一方对本协议任何一项的违约，都会给另一方带来不能弥补的损害，并且具有持续性，难以或不可能完全以金钱计算出受损程度，因此除按法律规定和本协议约定执行任何有关损害赔偿责任外，任何一方均有权采取合理的方式来减轻损失，包括但不限于指定措施和限制使用的合理请求。

九、纠纷解决程序与管辖

1.对因本协议或本协议各方的权利和义务而发生的或与之有关的任何事项和争议、诉讼或程序,本协议双方均选择以下第种方式解决：

（1）向本协议签订地人民法院提请诉讼；

（2）向仲裁委员会申请仲裁。

2.若协议履行过程中双方发生诉讼或仲裁，在诉讼或仲裁进行期间，除正在进行诉讼或仲裁的部分或直接和实质性地受到诉讼或仲裁影响的条款外，本协议其余条款应当继续履行。

十、其他

1.本协议自甲乙双方法定代表人或授权代表签字盖章之日起生效，且未经双方书面协议不得补充或修改。本协议签署、履行、解释和争议解决均适用中华人民共和国法律。

2.本协议一式份，双方各执份，具有同等法律效力。

（以下无正文）

甲　　方:（盖章）　　乙　　方:（盖章）

法定代表人/授权代表：　　法定代表人/授权代表：

日　　期:　　日　　期:

参 考 文 献

[1] 《中华人民共和国反不正当竞争法》

[2] 《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》（法释〔2020〕7号）

[3] 《中央企业商业秘密保护暂行规定》（国务院国有资产监督管理委员会〔2020〕第41号）

[4] GB/T1.1 标准化工作导则第1部分：标准的结构和编写

[5] 《商业秘密资产管理（2016）——信息资产管理指南》马克.R.哈里根，理查德.F.韦加德著. 北京：知识产权出版社，2017.10

[6] T/PPAC 701—2021 企业商业秘密管理规范

[7] DB33/T 2273—2020 商业秘密保护管理与服务规范

[8] DB34/T 4317—2022 商业秘密保护规范

[9] DB21/T 3659—2022 商业秘密保护管理规范

[10] DB11/T 2156-2023 城市副中心 商业秘密保护指南