# 低空经济产业

## 商业秘密保护工作指引

深圳市市场监督管理局

2025年12月

# 目　录

# 1 综述

## 1.1 低空经济产业概述

低空经济是指以民用有人驾驶和无人驾驶航空器在低空空域内的各类飞行活动为牵引，辐射带动相关领域融合发展的综合经济形态。低空经济产业链上游是低空经济发展的基石，聚焦为低空飞行器提供核心硬件与技术支撑，包括原材料、航电系统、飞控系统、零部件、任务载荷等；产业链中游是低空经济的核心载体，连接上游技术与下游应用，包括 eVTOL、无人机、新型低空飞行器等低空飞行器整机制造、空域管理与服务等；下游是整个产业链的飞行应用层，主要包括各类低空飞行器应用场景及各类低空飞行器保障服务。

近年来，随着“低空+”赋能千行百业，低空经济已在城市治理、空中交通、应急救援、低空文旅等多个场景中崭露头角，丰富的应用实践推动全产业链资源加速集聚，并带动相关领域不断实现技术升级与模式变革。

深圳市作为全球低空经济产业“密度”最高的城市，近年来凭借雄厚的产业基础厚积薄发，全力打造全链条低空产业高地，全速竞飞全球“低空经济第一城”。据统计，目前，深圳已集聚 1900 余家低空经济产业链企业，消费级无人机占全球市场 70%，工业级无人机占全球市场 50%，2024 年低空经济年产值超过 900 亿元，形成全球领先优势。

## 1.2 低空经济产业商业秘密保护的重要性

在上述背景下，低空经济产业创新成果不断涌现，商业秘密作为各创新主体核心竞争力的体现，其保护工作至关重要。低空经济产业的商业秘密涵盖无人机技术、飞行算法、商业模式及运营数据等关键信息，是相关

创新主体的核心命脉，直接决定了其在技术上的领先性、市场中的竞争力以及商业价值。这些信息和数据一旦泄露，可能导致技术被复制、市场被抢占、投资流失甚至面临法律诉讼等严峻风险。因此，建立健全商业秘密保护体系，对技术信息和经营信息实施全方位保护，不仅有助于激励创新主体持续投入研发、全力攻坚关键核心技术，更能有效维护公平竞争秩序，构筑产业安全底座，促进低空经济产业的可持续发展。

### 1.3 低空经济产业商业秘密的特点

1.高技术性。作为新兴科技产业，低空经济产业的商业秘密通常涉及高度专业的科学和技术信息，主要集中在无人机飞控系统、智能导航算法等高科技领域，专业性强、研发投入大，而且迭代更新速度极快，使得商业秘密的保护面临更高的要求。

2.场景依赖性。低空经济产业的商业秘密价值与其具体应用场景深度融合，不同应用领域如物流配送、应急救援等所需的核心技术参数和运营模式存在显著差异，要求相关创新主体在保护商业秘密时需充分考虑具体业务场景的特殊需求。

3.时效性。由于技术更新迭代快、商业模式容易被模仿，低空经济产业的商业秘密可能随时间推移而失去价值。一项核心技术可能在较短时间内就会被新一代技术所取代，这要求相关创新主体必须建立快速响应与持续更新的保护机制。

4.全链条覆盖。低空经济产业的商业秘密覆盖研发设计、生产制造到运营服务与保障等全产业链环节。无论是核心零部件的供应链信息，还是终端用户的运营数据，都可能构成具有商业价值的秘密信息，这要求企业建立贯穿整个业务环节的商业秘密保护体系。

5.敏感性。低空经济产业的商业秘密具有显著的数据敏感性特征，其核心数据不仅涵盖飞控算法、测试数据等技术信息，还包括用户信息、运营动态等经营信息。这些数据既涉及相关创新主体核心竞争力，又可能关联国家安全、公共安全和个人隐私。同时，低空经济涉及空域安全、跨境数据等特殊监管要求，商业秘密保护需要平衡商业利益和监管要求。

6.军民融合的特殊性。部分低空经济核心技术具有显著的军民两用特征，使得商业秘密保护不仅关乎相关创新主体自身利益，还涉及国家安全考量，这要求相关创新主体在保护商业秘密时必须兼顾商业价值和国家安全，对可转为军用或受出口管制的低空技术[1]在商业秘密定密前同步进行“出口管制合规筛查”。

## 1.4 主要内容和制定目的

本指引依据《中华人民共和国反不正当竞争法》以及深圳市《企业商业秘密管理规范》《科研机构商业秘密保护管理规范》等地方标准的基本原则和要求，在遵循法律理论和总结实务经验的基础上制定。涵盖商业秘密的确定、管理、维权等事前、事中、事后全流程的实务操作内容，具体包括如何有效识别与界定商业秘密，如何健全内部商业秘密保护体系、如何防范侵犯他人商业秘密，以及遭遇商业秘密侵权时如何维权等。

本指引充分结合低空经济产业的特点，提供更具针对性的商业秘密保护策略，旨在引导相关创新主体强化商业秘密的自我保护和合规管理，有效防范商业秘密泄露或侵权风险，全面激发我市低空经济产业全产业链创新活力。

诚挚建议低空经济产业相关创新主体认真研读本指引，积极采纳其中

[1] 具体可遵循《中华人民共和国出口管制法》及商务部 海关总署 国家国防科工局 中央军委装备发展部公告 2023 年第 28 号 关于对部分无人机实施临时出口管制的公告要求。

的实操建议，逐步构建系统、完善的商业秘密保护体系，将商业秘密管理贯彻到经营活动的各个环节，从而降低商业秘密泄露风险，并避免侵犯他人商业秘密，共同维护公平竞争的市场环境。

同时，需要注意的是，本指引为指导性文件，不具有行政强制力。在具体实务操作中，应遵循最新法律法规、司法解释和规范性文件，并充分分析主体的差异性和实际需求，实施有针对性的保护策略。相关信息涉及国家秘密的，须遵照《中华人民共和国保守国家秘密法》相关规定执行。

## 2 商业秘密的确定

根据《中华人民共和国反不正当竞争法》（2025 年修订）第十条，商业秘密指不为公众所知悉、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。

商业信息要想被行政机关或司法机关认定为商业秘密，需满足秘密性、价值性、保密性三个特征。秘密性，即指有关信息在侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得。价值性，即有关信息因不为公众所知悉而具有现实的或者潜在的商业价值。保密性即指权利人为防止商业秘密泄露，在侵权行为发生以前所采取的合理保密措施[2]。秘密性、价值性、保密性为商业秘密的法定构成要件，三者缺一不可。因此，准确界定自身商业秘密的范围，并事前采取相应的保密措施，是侵权行为发生后能够有效维权的基石和关键。

本章围绕商业秘密的收集、识别、确定、变更、解密、销毁等各个环节提供实操指引，并结合走访调研情况，对低空基础设施建设、低空飞行器制造、低空经济运营服务商等不同创新主体的商业秘密内容列出参考清单，以指引相关主体准确界定自身商业秘密，筑牢维权基础。

### 2.1 收集商业信息

商业秘密管理部门应确定商业信息的收集范围，根据收集范围确定承担收集工作的部门，并指定各部门保密员。总体来说，收集范围包括：

[2] 根据《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》第六条，具有下列情形之一，在正常情况下足以防止商业秘密泄露的，应当认定权利人采取了相应保密措施：a)签订保密协议或者在合同中约定保密义务的；b)通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；c)对涉密的厂房、车间、生物安全实验室等生产经营场所限制来访者或者进行区分管理的；d)以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；e)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、复制等措施的；f)要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；g)采取其他合理保密措施的。

涉密技术信息：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；技术信息可以是一项完整的技术方案，也可以是一项完整技术方案中的一个或若干个相对独立的技术要点。

涉密经营信息：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、客户信息、数据等信息；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。经营信息可以是一个完整的经营方案，也可以是经营方案中若干相对独立的信息要素个体或组合。所有可能给权利人带来经济利益或竞争优势的非技术类信息，都可以成为经营信息。

## 2.2 识别商业秘密

保密员应根据商业信息是否为公众所知悉、是否具有商业价值，定期/不定期识别研发、生产、经营过程中产生的技术信息和经营信息等商业秘密。识别周期参考如下方式确定：技术信息识别周期根据不同研发项目的完结节点确定，其他即时性信息（如市场信息、客户信息等）识别周期以周/月为单位确定。

保密员宜参考如下因素初步确定技术信息为商业秘密：

a)反向工程破解难易程度及技术生命周期持续性，破解难度越高、技术生命周期越长则商业秘密属性越显著；

b)反向工程所需时间成本与资金投入越高，则该技术信息越可能具备商业秘密价值。

根据《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》第四条，商业秘密应确认其不为公众所知悉，下列信息不应作

为商业秘密保护：

a)该信息在所属领域属于一般常识或者行业惯例的；如无人机飞行原理、无人机系统组成等。

b)该信息仅涉及产品的尺寸、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；如无人机外观、机身尺寸、布局、组成部分、机臂数量与折叠方式等信息。

c)该信息已经在公开出版物或者其他媒体上公开披露的；如在公开网站、杂志等上公开发表的产品性能、技术特点等。

d)该信息已通过公开的报告会、展览等方式公开的；如在航展、技术峰会中展示的无人机载重、续航时间、平飞速度、任务载荷接口类型等。

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；如通过第三方专业测评机构公开的在不同环境下的抗干扰能力等；如按运行安全规范，需实时对外广播及发布的信息。

特别说明的是：若上述信息经特定组合、编排或系统化处理后，所形成的信息要素组合不为公众知悉，仍然符合商业秘密的构成要件，则该组合整体应作为商业秘密予以保护。

## 2.3 确定商业秘密

由产生商业秘密的业务部门提出拟确定的密点、密级、保密期限、知悉范围等；经商业秘密管理部门审核并报领导审批后确定。

**低空基础设施建设**相关创新主体宜按照需求分析、概念设计、仿真验证、环境评估、施工规划、材料采购、施工建设和验收交付等环节确定商业秘密。

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| **需求分析** | 合作方信息、项目建设目的与意图、合作方向与模式、调研数据、需 |

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| | 求分析报告、初步技术构想、初步投资估算、资源配置、预期收益模型、回报周期、未公开的选址评估模型、基础设施布局规划等。 |
| **概念设计** | 总体设计方案：通信、导航、气象、数据管理等子系统的集成方式、关键设备性能指标与参数、通用机场、低空飞行器起降平台、充电站、试飞场地、低空通信基站等低空经济基础设施三维模型、结构设计方案、技术难题解决方案、技术融合方案等。 |
| | 创新性设计理念与算法：新型材料应用、多系统集成的接口构想、无人机路径规划核心算法、流量优化模型、冲突解脱逻辑等。 |
| | 硬件设计与集成方案：硬件设计图纸、设备结构与电路、核心部件选型与供应链信息、系统集成与部署方案等。 |
| | 商业模式：成本效益分析模型、商业模式、市场拓展计划、合作框架、采购成本与预算、潜在风险及应对方案等。 |
| **仿真验证** | 验证方案、仿真模型与算法、仿真过程与优化诀窍、基准数据、模型参数与校准数据、验证环境、仿真验证流程、性能瓶颈分析报告、性能优化策略、优化算法、解决方案等。 |
| **环境评估** | 环境评估指标、阈值、评估模型、方法、工具、测试数据及报告、环保认证数据、应急超标处置方案、技术解决方案等。 |
| **施工规划** | 规划方案、进度计划、施工工艺参数、专项技术方案、资源调度方案、安全控制方案、应急预案、风险管控策略、施工成本控制方案、分包商选择策略、质量检测方案等。 |
| **材料采购** | 采购策略、采购计划、采购清单、库存管理、材料技术规格参数、设备性能参数、独家设备的采购渠道、供应商信息、价格成本、合同条款等。 |
| **施工建设** | 施工方案、施工工艺、施工图纸、施工记录、项目进度控制、技术参数、实时资源调度信息、工程管理数据、质量控制标准、检测方法、分包商合作细节、施工风险应对、应急方案、施工成本等。 |
| **验收交付** | 验收标准、验收方法与工具、全套竣工图纸、核心系统的配置手册、运维手册、交付风险的规避策略等。 |

**低空飞行器制造**相关创新主体宜按照市场调研、概念设计、适航审定、详细设计、原型机验证、工艺开发、生产（含试生产）、销售与交付、售后与迭代优化等环节确定商业秘密。

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| **市场调研** | 产品的市场定位、目标用户、目标区域、预计进入时间、产品用途、 |

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| | 调研需求、市场进入策略、竞品分析报告、差异化竞争策略、商业模式、定价策略、投融资策略、初步技术路线、供应链等。 |
| **概念设计** | 初始设计方案、设计图纸、设计参数、设计理念、可行性论证分析报告及数据等。 |
| **适航审定** | 适航证申请书、技术资料、适航性评审和检查记录、适航检查报告、运行风险评估报告、空域使用审批文件及航线规划方案、安全测试验证文件等。 |
| **详细设计** | 总体设计图纸与模型、动力系统、飞控系统等子系统核心技术参数、设计规范、设计结构、功能架构、外形设计参数、结构设计参数、专属材料与工艺规范、潜在风险解决方案等。 |
| **原型机验证** | 飞行性能、结构载荷数据、环境适应性、核心部件实测数据、未公开功能、性能测试报告、测试故障与报告、优化方案、测试设备与方法等。 |
| **工艺开发** | 质量检测工艺、装配与调试工艺、金属加工工艺、复合材料的独家配方与处理工艺、系统集成工艺、生产设备的技术参数、模具设计图纸、专有技术诀窍、实验与测试数据等。 |
| **生产（含试生产）** | 生产工艺、工艺参数、生产设备、设备型号、设备参数、关键物料、物料型号/规格、采购需求文件、供应商名录、采购合同、生产计划、质量要求、执行标准、验收标准、产品良率、工序耗时、物料损耗率、废品处理、单台产品成本及利润等。 |
| **销售及交付** | 经销商名录、定价机制、代销协议、招投标文件、销售渠道、销售方案、客户交易习惯、存货量、客户信息等。 |
| **售后及迭代优化** | 故障统计数据、客户隐性需求、维修技术手册、迭代优化方案等。 |

**低空经济运营服务商**针对特定场景提供服务时，相关创新主体可围绕场景应用需求调研、空域与航线管理、运营服务与保障、安全监管等核心环节确定商业秘密。

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| **场景应用** | 低空场景生态拓展蓝图、市场定价模型与盈利模式、客户信息、运营流程、技术集成方案、合作细节等。以下仅列举了四种常见的低空经济应用场景。在低空经济的其他应用场景中，相关信息能否构成商业秘密，宜依据其是否满足商业秘密的法定构成要件进行判定。 |
| | 物流配送：未公开的无人机路径规划信息、配送调度算法、特种货物 |

| 环节 | 商业秘密（未公开信息） |
| --- | --- |
| | 处理方案、客户画像与需求预测数据等。 |
| | 空中交通：乘客流量预测算法、冗余安全设计与故障处置预案、票务动态定价模型、低空飞行器客舱人机交互设计等。 |
| | 农业植保：精准变量施药算法、病虫害识别模型、作物生长状况评估算法、全流程自动化技术诀窍、运营模式等。 |
| | 应急巡检：自动化巡检航线与隐患识别标准、诊断报告生成系统、专用巡检传感器集成与数据分析算法等。 |
| **空域与航线管理** | 内部用于提升自身运营效率的技术与策略，如专有的航线划设方案、冲突解脱算法、低空作业能效优化模型、抗干扰技术、运力调度算法、空域实时调度信息等。 |
| **运营服务与保障** | 实时航线数据、任务调度日志、飞行轨迹热力图、飞行数据、通信监视数据、气象数据、数据传输与存储的方法、工具与算法、服务时段偏好、飞行任务完成率、设备维护方案、远程监控系统、定价策略、服务策略、客户需求分析、市场调研报告、事故处理流程、净空保护区域的相关空域数据，以及应急响应预案等。 |
| **安全监管** | 与监管部门的非公开沟通文件、合规策略、风险评估模型与方法、应急处置流程与预案、数据安全与隐私保护方案等。 |

## 2.4 密级划分

商业秘密管理部门应将商业秘密进行分级管理，依据商业秘密的秘密性、价值性以及泄密对本单位经济利益和竞争优势的损害程度，可将密级分为核心商业秘密、重要商业秘密、普通商业秘密三级。为便于操作，也可将商业秘密简化为两级，即核心商业秘密和普通商业秘密。密级可采用形状结合文字的形式，例如：“★★★+核心商秘”“★★+重要商秘”“★+普通商秘”。定期对商业秘密密级复评和动态调整，根据商业秘密级别，采取不同保密措施。密级可参考以下内容划分：

a)涉密信息所具有的经济价值；

b)产生涉密信息投入的成本；

c)涉密信息的重要程度；

d)竞争对手获取涉密信息后可能产生的价值；

e)涉密信息泄露后可能造成的经济损失；

f)涉密信息泄露后可能承担的法律责任；

g)涉密信息在内部的知悉范围。

## 2.5 保密期限

根据商业秘密的密级、商业秘密的生命周期、技术迭代周期、技术成熟度、潜在价值、市场需求等因素设定商业秘密的保密期限。一般情况下，涉密信息的解密期限可以确定的，可以“年”“月”“日”计，不可预见期限的，可定为“长期”或“公开前”。

保密条款的效力应当在合同期限届满后一个时期仍然有效，直至涉密信息失去保密的必要，因此保密期限一般要长于合同期限。合同中应特别明确，在保密期限内，对于由一方向另一方透露的任何改进，保密期限需重新起计。合同提前终止，或部分条款无效或不能执行的情况下，保密条款的效力不受影响。

## 2.6 变更

商业秘密管理部门应根据经营实际，调整商业秘密的保密状态、密级、保密期限、知悉范围等信息。

涉密信息有关事项如需变更的，应履行审核审批程序。

## 2.7 解密

相关创新主体的商业秘密一旦出现下列任一情形，保密员应及时向商业秘密管理部门报备，商业秘密管理部门可采取移除密级标识、解密电子

文件等措施予以解密：

a)经评估认定该商业秘密事项已失去保护意义，不再具备秘密性、价值性或保密性；

b)保密期限届满或该信息已通过合法渠道公开；

c)因其他特定原因导致商业秘密被公开的。

商业秘密的解密措施包括但不限于：

a)撤销涉密物理区域的管控措施并进行清理，解除逻辑区域访问限制；

b)消除原有密级标识，或根据实际情况更新为非涉密标识；

c)电子文档的密码解除或访问权限开放；

d)其他方式。

## 2.8 销毁

凡涉及商业秘密的文件（含副本）、资料、电子信息、载体及物品等，均需履行销毁程序，严禁随意处置。由保密员列出销毁清单，详细注明物品名称、数量、密级、形成日期等信息，履行清点、登记手续后，由商业秘密管理部门组织统一销毁。

商业秘密的销毁全过程应在商业秘密管理部门的监督下进行，确保销毁行为规范、彻底，监督人员需对销毁结果签字确认。

销毁标准可参照以下方式进行：

纸质类：必须通过专业设备粉碎至无法复原的颗粒状，或采用焚烧方式彻底销毁，杜绝信息复原可能。

电子类：必须使用专业擦除工具进行不可恢复的永久删除，对存储介质（如硬盘、U 盘等），必要时采取物理破坏，如粉碎、消磁方式确保信息无法恢复。对于专用科研设备，建立信息清除流程，在设备停用、移交

或报废前，由专业人员对存储的涉密信息进行针对性彻底清除，确保信息不可恢复。

实物类：产品原型、零部件、模具等可采用碾压、切割、熔融等方式，使其失去原有功能和形态，无法被识别和复用。

## 2.9 商业秘密清单

相关创新主体应建立商业秘密清单，清单内容应覆盖：

a)商业秘密名称与核心主题，概括秘密内容与核心价值；

b)明确的密级设定（如核心、重要、普通）及具体保密期限；

c)所属部门及权属信息，清晰界定管理责任主体与权利归属；

d)限定的知悉范围，明确哪些部门或岗位可接触该商业秘密；

e)涉密人员名单及其对应的访问权限，实现人员与权限的精准匹配；

f)商业秘密在内部流转、外部交互等场景下的具体要求，包括传递方式、审批流程等；

g)存储方式与物理/电子存放地点，确保可追溯；

h)相关审批文件的索引或编号，便于快速查阅审批记录。

## 3 商业秘密的管理

商业秘密管理是一项系统工程。本章对管理制度、管理机构、侵权风险防控管理、应急管理等方面提出策略建议，并对人员、涉密区域、涉密载体等不同对象，以及研发、销售、财务、外部合作等关键环节的商业秘密管理提供实操方法，指引创新主体构建全方位的商业秘密内部管理框架。

### 3.1 管理制度

相关创新主体应根据经营情况，建立完善商业秘密保护管理制度体系，确保商业秘密保护与管理工作有章可循。包括但不限于：

a)商业秘密保护管理制度，作为统筹性文件明确商业秘密管理工作的目标、方针、适用范围、策略和原则等；

b)涉密文件资料（物资）管理制度，规范涉密载体的生成、传递、使用、保存及销毁等全流程管理；

c)研发项目及外部合作管理制度，针对研发过程及对外合作中的信息交互，设定保密要求与风险防控措施；

d)涉密专用设备管理制度，对承载商业秘密的设备及计算机终端，从采购、使用、维护到报废的全生命周期实施安全管控；

e)网络安全管理制度，明确涉密信息在互联网环境下传输、存储的安全规范，防范网络泄露风险；

f)涉密区域（场所）管理制度，划定涉密区域等级，设定出入权限与管理规范，保障物理空间内的信息安全；

g)涉密人员管理制度，涵盖涉密人员的聘用、培训、考核、离岗等环节，强化人员保密责任与行为约束；

h)对外交流及宣传管理制度，规范对外信息披露行为，明确交流与宣

传中商业秘密的保护边界；

i)客户名单管理制度，规范客户名单的创建、存储、使用、传输及销毁全过程，以保障商业秘密与客户隐私安全，维护核心竞争优势；

j)商业秘密泄露事件处置管理制度，建立泄密事件的报告、调查、处置及善后流程，提升应急响应能力。

### 3.2 管理机构

相关创新主体可根据实际经营情况，设置专门的商业秘密管理部门或由具备商业秘密保护职能的部门承担商业秘密保护与管理工作，并明确其职责。小微企业或商业秘密相对较少的创新主体，也可以不设部门，而是指定专门人员负责管理。

商业秘密管理部门应配备专职负责人，或指定如法务、研发、人力资源等部门负责人兼任，也可由最高管理者直接负责。各业务部门应至少抽派 1 名人员担任本部门保密员，协助落实商业秘密保护与管理的具体工作。各相关部门应配合商业秘密管理部门开展本部门职责范围内商业秘密的保护和管理工作，落实商业秘密保护制度，并结合自身业务特点针对性防范商业秘密泄露或侵权风险，共同形成覆盖全流程、全领域的商业秘密保护合力。同时，各部门应及时向商业秘密管理部门反馈工作中发现的问题与风险隐患，以便统筹协调解决，保障商业秘密保护体系的有效运转。

企业的分支机构、子公司及关联企业，可参照主体企业的组织架构模式，相应设置商业秘密管理部门，确保商业秘密管理体系在集团范围内的一致性与有效性。

商业秘密管理部门的工作职责包括但不限于下列内容：

a)统筹负责商业秘密保护的管理工作，确保各项工作有序开展；

b)牵头组织制定商业秘密保护与管理的相关制度及具体执行流程，为保密工作提供制度依据；

c)研究确定商业秘密保护的范围、密级划分、保密期限及涉密区域等，以及生产经营各环节中商业秘密保护的技术防护措施等关键事项；

d)定期对商业秘密进行评估，根据评估结果组织开展商业秘密的更新、解密及销毁工作，确保商业秘密保护与管理工作的动态性与时效性；

e)组织开展员工保密宣传教育活动，提升全员保密意识与相关技能；

f)指导并组织各部门落实商业秘密保护与管理的各项具体措施；

g)监督检查各部门商业秘密保护与管理工作的执行情况，对发现的问题及时提出整改要求，并跟踪督促整改到位；

h)负责处理泄密事件，协同有关部门完成证据的搜集、整理、举证以及协助调查取证等工作，保障维权工作顺利进行；

i)其他与商业秘密保护与管理相关的工作。

### 3.3 人员管理

#### 3.3.1 入职管理

相关创新主体可根据自身规章制度，与新入职、转岗到涉密岗位的人员签订与岗位工作内容相适应的保密协议，并约定保密范围、双方权利义务、保密期限、违约责任等。

员工入职前，可通过章程、制度、员工手册以及书面通知等方式，确保员工知悉内部商业秘密的范围及相应的行为界限，并保存相应记录。

高级管理人员、核心技术人员及其他负有保密义务人员（如职业经理人、技术、采购、销售等涉密重点岗位人员）入职时，应签订竞业限制协议，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，以强化对核心商业秘密的保护。

针对新入职员工，开展商业秘密基础培训，宜包括以下几个方面：

a)商业秘密基础知识；

b)员工的商业秘密保护权利和义务；

c)常见的泄露或侵害企业商业秘密的行为及相关案例；

d)侵害商业秘密可能会承担的法律责任。

### 3.3.2 履职管理

制定涉密岗位及涉密人员清单，包括涉密人员姓名、岗位、所属部门、商业秘密接触权限、涉密等级等信息，并根据岗位变动及人员流动情况及时更新，确保清单的准确性与时效性，为精准化保密管理提供基础依据。

针对涉密人员，商业秘密管理部门应会同业务部门定期监督检查，审核其保密职责履行情况，发现异常情况，应及时上报处置。

实施严格的分级授权制度，一般情况下，知悉范围应按照“最小知悉范围”原则，明确限定到具体的业务部门、具体岗位和具体人员，并按照密级实行分类管理。涉密人员原则上不得跨级别和跨部门接触和知悉保密权限以外的商业秘密。如果涉密人员因工作需要必须知悉保密权限以外的商业秘密，应报请业务主管部门和商业秘密管理部门批准并备案。

根据员工接触项目所涉及的商业秘密信息，要求其签署保密承诺书。

定期开展日常保密培训工作，培训内容主要包括：

a)商业秘密基础知识培训：深入解读商业秘密的定义、范围、法律保护依据，明确泄露商业秘密的法律责任和后果，重点剖析低空经济产业链各环节的泄密风险点，提高员工商业秘密保护意识；

b)岗位保密要求培训：结合不同岗位的性质与职责划分，详细讲解其对应的商业秘密保护范围、员工操作权限及具体行为规范，确保员工清晰

掌握岗位保密要点；针对研发人员、技术人员等核心涉密岗位，重点强化对研发成果的保密意识与实操规范，同时建立与管理人员、市场人员等的差异化培训体系，通过模拟泄密风险环节提升实战应对能力；

c)日常信息安全操作培训：涵盖电子文档加密标准、存储设备管理规范、办公区域安全准则及远程办公保密要求等实操内容，提升员工日常工作中的信息安全操作能力；

d)对外交流保密：规范员工在商务洽谈、学术交流、展会活动等场合的言行，明确禁止披露的信息范畴，防范因疏忽导致的无意泄密；

e)应急处理培训：指导员工识别可疑行为和泄密风险，熟练掌握泄密事件的报告流程及基础应急处置方法，确保在突发情况下能快速响应；

f)典型案例教育：分析低空经济行业商业秘密侵权案例，以实际教训强化员工的保密警觉性，筑牢思想防线。

同时，可采取发放员工保密管理手册、召开全体员工保密动员会、张贴保密宣传标语等方式开展员工保密宣传，并形成培训记录；若培训结束后进行考核的，需保存培训相关考核资料。

### 3.3.3 离职管理

在员工提出离职意向后，由其直属经理和商业秘密管理部门共同进行初步评估，判断该员工是否为核心涉密人员，并确定后续措施的严格等级。

离职员工在启动离职流程后须填写并提交《涉密信息自查清单》，要求员工系统性地列明其在职期间，尤其是离职前一年内，所直接或间接接触、处理、创建的所有商业秘密。

对离职员工进行离职面谈，并结合《涉密信息自查清单》，逐一、明确地重申清单所列各项信息的保密要求。告知员工保密义务不因劳动合同的解除或终止而失效，强调违反保密规定将承担的法律责任与后果，确保

员工充分知晓离职后的保密责任。

及时收回离职员工的所有权限，包括计算机系统、网络、门禁、文件存储设备等。同时，及时通知与离职员工有关的供应商、客户、合作单位等，有序推进业务交接，保障合作关系的稳定性与信息安全。

对离职员工的办公设备进行检查，具体内容包括但不限于：检查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；检查工作邮箱的邮件收发记录；离职前一定期限内的涉密文档、数据的查看和使用情况等。

涉密岗位员工离职前，应提醒离职员工主动移交一切涉密载体和物品，包括纸质文件、电子存储介质、涉密设备等，并制定详细的离职交接清单，安排专人逐项核对确认，确保交接工作完整无误。

对涉密岗位员工离职后的去向进行定期追踪，掌握涉密岗位员工离职后履行保密承诺书、竞业限制协议的情况，及时掌握涉密信息泄露或者不当使用的线索，一旦发现异常，及时采取应对措施。

### 3.4 涉密区域管理

涉密区域指可以接触到商业秘密信息的一切场所，包括但不限于企业及科研机构园区、核心研发区、厂房、车间、质量控制与分析区、实验室、关键物料存储区、办公室、保密室、档案室、机房、外部关联场所、用户现场等。

涉密区域应与其他工作区域相互隔离，实施差异化管理。配置安全防护和监控设施，设置明显的警示隔离标志，不同区域之间的人员流动需要符合保密隔离的制度要求。

涉密区域采用物理隔离，仅向必要人员开放，非授权人员包括外部访

客、非相关岗位员工等需经多级审批方可进入，且全程由专人陪同，禁止携带具有存储、拍摄功能的电子设备。

访问控制。采用人脸识别、指纹验证和 IC 卡等技术手段控制人员进出涉密区域。形成访问日志并设置异常访问预警机制。

监控系统。在实验室与生产车间等敏感关键区域部署具备红外夜视功能的全景监控系统，实现 24 小时无间断监控，精准记录人员活动轨迹与操作行为，确保对涉密场所的全时段、无死角管控。监控视频资料加密存储，确保影像的完整性和不可篡改性。

### 3.4.1 研发中心管理

a)研发中心应独立设置，与普通办公区域物理隔离，采用门禁系统（如刷卡、指纹或人脸识别）控制进出；

b)研发实验室应配备视频监控、信号屏蔽装置；

c)研发设备（如 3D 打印机、仿真测试台等）需固定编号管理，禁止私自携带出研发区域；

d)研发人员、技术人员入职时应签署保密协议，接受保密教育培训和监督检查；

e)研发数据需加密存储，严禁将涉密研发资料带离指定工作场所或在个人电子设备上进行存储、使用及传输；

f)研发资料严禁通过互联网、社交媒体等渠道传递；

g)技术人员、研发人员对外参加科学技术交流合作、商务活动前，需向商业秘密管理部门报备，明确合作交流内容不涉及商业秘密保护范围。

### 3.4.2 数据中心管理

a)飞行数据，如航迹、传感器日志等存储于加密固态硬盘；明确数据存储格式要求，确保可追溯性和完整性验证；采用加密通信或算法传输数

据，避免无线电侦测截获；所有涉密低空飞行器承载的低空经济数据严禁通过公共互联网和非受控端口进行传输，并根据数据类型和敏感程度实施分级管理；

b)建立数据安全防护系统，包括物理、网络、服务器与应用、终端、移动存储介质和信息导入导出等方面。数据安全应与信息系统安全同步规划与建设，两者缺一不可；

c)数据库访问需启用动态令牌和生物识别双重认证，做好 24 小时视频监控，操作日志全量留存并定期审计；

d)建立数据分类分级管理体系，按核心数据、重要数据、一般数据实施差异化访问权限控制；

e)严禁在连接互联网的计算机或手机上存储、处理数据；不使用微信、微博、短信、邮件、云盘、网盘等互联网途径存储、处理、传输数据；

f)第三方运维服务商需签订保密协议，并对其数据与系统的访问权限实施严格的时效与范围管控。

### 3.4.3 生产区域管理

a)复合材料成型、系统装配等关键工艺在独立车间保密进行，非相关人员不得进入；车间布局实现工艺环节物理分隔，避免交叉泄密风险；

b)生产车间需建立生产工艺文件清单，实时更新并存档于指定保密文件柜中，确保清单与实物一致；

c)每个车间应当及时记录接收、转出、替换、借阅及归还工艺文件情况，严禁擅自复制或带离工作区域。确因工作需要复制或外借的，需经车间负责人审批并留存书面申请记录；

d)生产设备需设置操作权限，关键参数加密存储，防止非法拷贝；

e)任何摄影、摄像及录音设备均不得带入生产车间，禁止其拍照或录

音泄露生产工艺；因安全生产，需要拍摄的，应制定相应细项要求并严格执行；

f)严禁将生产现场的产品、半成品、原材料、配方等一切与产品生产相关的物品带离生产区域。

### 3.4.4 试飞基地管理

a)试飞基地实行封闭式管理，未经授权人员不得进入；

b)划设“禁飞缓冲区”，配备干扰监测系统，防止外部无人机违规拍摄；

c)试飞跑道、停机坪等核心区域安装雷达或报警装置，未经授权的人员或设备进入即触发应急响应；

d)试飞计划采用“最小化知情范围”和任务分解管理模式，禁止对外公开具体时间、坐标及飞行参数；

e)试飞员、地勤人员需通过背景审查，禁止携带手机、相机等摄录设备进入场地。

### 3.4.5 低空试验区域管理

a)针对无人机测试场、风洞等开放空间，根据“最小授权”和“业务必需”原则，将人员权限划分为核心研发、试验操作、外围保障等不同等级，构建以身份认证为核心的多维物理安全体系；

b)在试验期间，对试验空域进行临时性净空管理，禁止未经授权的其他低空飞行器进入，防止空中窥探与数据截获；

c)对地面指挥控制中心、数据中心等核心涉密点位，配备可移动的屏蔽帐篷或部署在固定建筑物内，防止关键操作与内部交谈被窃听或窥视；

d)根据试验的保密级别，评估并配备必要的电磁屏蔽或信号干扰设备，防止试验数据的无线传输信号被外部截获；

e)试验结束后，核对和回收所有涉密载体，确保无一遗漏。

### 3.4.6 空域场景差异化管理

低空经济涉及多样化场景应用，需针对不同场景制定差异化商业秘密保护管理策略：

a)城市空域，应加强防窃密与防干扰能力。针对政府机关、军事驻地等敏感区域，主动规避在相关设施周边执行飞行任务；通过加密技术保障飞行路径与数据传输安全；使用专用通信频段以降低公共频段干扰风险；配备自毁芯片或远程锁机功能，确保在设备丢失或失控情况下关键数据不被泄露；

b)农村、远郊及山林等偏远地区空域，加固通信安全，减少对公共移动网络的依赖，避免通信经第三方基站中转，降低信号被截获与窃听的风险；低空飞行器加装 GPS 追踪+远程锁机功能，失联后自动触发数据擦除；采用低噪音和伪装涂装，避免引起无关人员注意；

c)跨境空域，提前与边防、海事部门建立联动机制，遭遇干扰时可快速验证身份；敏感数据存储本地化，跨境传输前需完成安全评估并脱敏；

d)特殊空域，如军事管制区、核设施周边空域等区域及专用航线的管理需融合政策合规性与技术保密性，防止未授权使用与参数泄露。特殊空域的三维坐标需采用加密技术存储，实际使用时通过算法动态还原真实位置。临时开放的特殊空域，其开放时段、申请渠道、审批权限等信息，需限定在“最小知悉范围”内，且仅通过加密专线传递。涉密航线，飞行前由地面系统生成动态航线参数，通过加密通道传输至低空飞行器，任务结束后立即废止参数。

## 3.5 涉密载体管理

涉密载体是指以文字、数据、符号、图形、图像、视频和音频等方式记载和存储商业秘密信息的纸介质、电子文件、光介质、电磁介质、设备与产品等各类物质。[3]

### 3.5.1 纸质文档

涉密纸质文档应存放于设置保密柜的保密室，实施严格的文件管理制度，由专人保管，并登记造册，定期根据清单清点。涉密纸质文档的使用宜采取以下管理措施：

a)涉密纸质文档原则上不应打印、扫描、传真和借阅，若确有使用需要的，应按权限或经过审批使用，并履行登记手续；

b)涉密纸质文档的复印件与原件的密级和保密期限相同；

c)根据涉密纸质文档传递的紧急程度和密级要求选择由专人携带、专用箱包/专车运输、机要邮政渠道传递和邮寄，避免使用普通邮政、普通传真机、非涉密网和互联网等邮递或传输涉密文件；

d)定期清查涉密纸质文档的使用情况。

### 3.5.2 电子文件

涉密电子文件应采用加密方式存储于授权的存储设备、应用系统或云存储空间，并定期备份。同时，涉密电子文件的收发应使用唯一出入口，对涉密数据流入流出行为审批。涉密电子文件的流转宜采取下列管理措施：

a)设置加密和签名；

b)指定专人解密；

---

[3] 注 1：纸介质是指传统的纸质涉密文件、书刊、图纸等。

注 2：电子文件是指以电子形式存储的文档或数据。

注 3：光介质是指利用激光原理写入和读取商业秘密的存储介质，包括 CD、VCD、DVD 等各类光盘。

注 4：电磁介质包括电子介质和磁介质两种，如各类闪存盘、计算机软盘、硬盘、磁盘、磁带等。

注 5：其他设备与产品是指直接含有，或通过观察、测试或分析等手段能够获取商业秘密信息的设备或产品，包括原材料、半成品、样品等。

c)限定文档的读写权限、打开次数和时限；

d)定期跟踪文档管理系统中涉密信息的操作日志，确保信息可追溯；

e)在文档首页、页眉、页脚、页面水印等处设置保密义务提醒；

f)通过内部局域网或加密网络通道对外传输；

g)其他认为有必要采取的管理措施。

应对涉密设备、数据库和各类应用系统及其账户实行权限管理，权限到期、人员转岗、项目或事项变更时应重新授权。权限宜按岗位职责或特定工作事项以“最小知悉范围”原则设定：

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、查看等权限及使用期限；

d)合理设定不同账户的互联网使用权限；

e)其他有必要设置权限的软件、系统或设备等。

### 3.5.3 涉密专用设备

对于存有涉密信息的专用设备，粘贴明显涉密标识。设备连接网络宜通过防火墙进行安全隔离，日常工作安排、任务下达、资料传递、信息交流等活动应在内部网络中进行。商业秘密管理部门应当协同网络管理业务部门负责内部网络系统的安全管理，并在网络后台持续监测员工搜索、浏览、下载、传输商业秘密的行为是否存在异常情况。

涉密专用设备宜采取以下保密管理措施：

a)设置不同涉密人员的操作权限；

b)建立涉密用户操作日志，实时记录并定期检查用户登录、获取信息和异常侵入等情况；

c)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；

d)设置信息加密系统，确保商业秘密均经过加密处理；

e)未经批准不应安装非授权软件，不应接入非授权网络；

f)在日常管理中区分并隔离涉密信息操作系统与非涉密信息操作系统，避免在两系统之间直接传输任何信息；

g)其他合适的保密管理措施。

所有存储在涉密计算机上的低空经济数据必须进行加密处理。根据数据分级，选择不同强度的加密算法。加密密钥由商业秘密管理部门统一生成、管理与分发，定期更换密钥，确保加密安全性。

内部涉及低空经济数据传输的网络应与外部网络实现物理隔离，构建独立的涉密内部网络。在涉密网络内，根据部门职能与数据流向，合理划分虚拟局域网，限制不同区域间的数据访问，减少数据泄露风险。对于外部数据传输，应采用高安全性的加密通道，确保传输过程的安全性和完整性。涉及重要数据时，可采取物理介质专人递送的方式，规避网络传输潜在风险。在对外提供数据前，须对敏感信息进行严格的脱敏处理，防止商业秘密外泄。

### 3.6 研发活动管理

对研发决策、立项、执行及成果转化全过程进行保密管理，并参照本指引文件采取保密措施，确保研发全链条信息安全。

研发决策阶段的保密管理应覆盖决策议题、会议纪要、决策内容、参会人员名单及决策过程记录文件等核心信息，所有决策文档须采用加密方式存储，严格限制访问权限。

研发立项环节的保密范围包括项目技术路线、核心研发内容、详细研

发计划、阶段里程碑节点、预算明细及研发团队人员构成等关键信息，需建立专项保密台账。

项目执行过程中的场所、研发和参与人员、外部协作、设备和原材料采购及使用、研发过程中形成的试验数据、半成品和样品、废弃物等，应予以保密管理和处理，建立研发物资全生命周期追踪系统，废弃物实施粉碎/消磁处理。

对于重要项目的研发活动，应遵循“最小知情范围”原则，与项目参与人员单独签订保密协议，明确对研发目标、主要技术指标、研发计划、参与人员信息、物品、场所等的特殊保密要求。

研发成果包括研发总结、研发报告、产品或设备、成果验收或检测、鉴定报告等，对于研发成果及记载研发成果信息的载体都应采取保密措施，技术文档类实施加密存储，实物类进行唯一标识与溯源管理，数据类通过区块链技术进行存证固化。研发成果确定归属于本单位的商业秘密，应按照本指引开展商业秘密管理工作。确定归属于员工或第三方的商业秘密，且该商业秘密与本单位相关的，本单位应与员工或第三方签署保密协议，要求员工或第三方履行保密义务。

### 3.7 销售管理

**客户信息管理。**对于由客户的名称、地址、联系方式以及交易习惯、意向、内容等区别于相关公知信息的特殊客户信息组成的客户名单，应按照本指引开展商业秘密管理工作。

**招投标管理。**对于涉及技术秘密的招投标方案、标书等文件，应开展商业秘密管理工作，防止技术流程、报价模式和评审细节的泄露。

**产品流通管理。**对于已上市且涉及技术秘密的产品，应当实施有效的

技术保护手段，以抵御通过反向工程获取商业秘密的风险，如采取一体化结构，产品拆解后技术秘密即被破坏。

### 3.8 财务管理

应对涉及商业秘密的财务信息进行严格管理，可采取以下措施：

防范员工在公共场所、非加密通讯渠道讨论涉密财务信息，不得在不利于保密的位置存放纸质涉密财务资料，外出携带涉密财务资料需经部门负责人书面批准，使用防拆封专用文件袋。

与财务相关的重要文件、软件、报告应设置密钥，指定专人保管，密钥密码定期更换。使用人不得泄露密码，并保证密钥和密码的使用安全。

对因工作原因需要查阅重大交易记录、重要财务数据的，查阅人应提出申请并逐级审批，审批流程全程电子留痕，系统自动生成日志，详细记录查阅人、查阅时间、查阅内容及审批情况等信息，便于追溯管理。

安排专人管理网银业务系统的交易数据，管理人员必须通过严格的资信调查。定期对网银业务系统的保密措施进行检查，包括系统权限设置、数据加密情况、操作日志记录等，确保网银业务系统信息的保密性与安全性。

### 3.9 外部合作管理

#### 3.9.1 信息发布管理

在广告宣传、成果展示等对外经营活动中，应建立严格的信息发布审查机制，防止涉密信息不当披露。对于涉及商业秘密的展示产品，须采取物理隔离（围挡）、关键部位遮盖、禁止拍摄等防护措施，确保商业秘密不被非法获取。

参加技术交流会、成果论证会等学术活动时，原则上不得展示涉密技术资料。确需展示的，应对材料进行密级标识，并仅限已签署保密协议的指定人员接收，活动结束后，须立即对展示材料进行回收，并详细登记备案回收情况，确保资料无遗漏。

通过专利、论文、新闻媒体等渠道公开发布信息前，应提前进行保密审查，由商业秘密管理部门会同业务部门对文稿内容进行全面核查，确保文稿内容不包含核心技术参数、关键工艺细节、特殊配方等商业秘密。

明确要求涉密岗位员工不得在互联网论坛、社交媒体、即时通讯工具等平台讨论或传播与工作相关的敏感信息，并纳入保密协议条款进行约束。

### 3.9.2 外部人员访问管理

外部人员进入，应出示证件并履行登记程序，佩戴与内部员工相区别的出入卡。

外部人员访问研发中心、数据中心、生产区域、试飞基地等涉密区域应经审批同意并进行登记，禁止录音、摄像、摄影、使用便携机、移动存储介质等设备，限制手机等器材的拍摄功能，安排专人全程陪同。

区分可参观区和禁止参观区。设置专门的参观路线以避开涉密区域，并采取好隐蔽措施。

### 3.9.3 技术合作管理

相关创新主体在开展合作研发、委托研发、技术授权及转让等活动时，应建立完善的商业秘密保护机制。

在开展技术合作前，应充分调查合作方的商业秘密管理能力，评估潜在侵权风险，核查其与竞争对手的合作关系，并与合作对象签订技术合作协议，在协议中宜约定：

a)商业秘密的权属划分、使用权限边界、日常管理责任及争议处理机

制等核心内容；

b)改进技术中的商业秘密权利归属，包括所有权、使用权、转让与许可权、收益权以及商业秘密成果归员工个人时的优先使用权等，并明确各方权利义务等内容；

c)对于联合研发过程中产生的中间成果，合作双方应承担与最终成果同等的保密义务。当一方需要使用中间成果时，使用方须填写《中间成果使用申请表》；

d)其他有必要约定的内容。

不同的合作对象，如科研机构、企业、高校等，应制定差异化的保密协议，明确己方的保密要求，并商定对方需配合的保密措施，如设立保密岗位、限制信息接触人员等。

在技术合作过程中，需定期对保密协议的履行情况进行监督检查，重点核查合作方对涉密信息的管理、使用是否符合约定。发现异常情况，及时排查，确有问题的，应及时采取补救措施。

### 3.9.4 会议及活动管理

在学术交流、行业展会等会议或其他活动中，宜采取保密措施，包括但不限于：

选择具有保密条件的场所，尽量避免使用远程视频、音频、电话会议等线上会议方式，如必须采用的，应采取会议密码、屏幕水印等措施。

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；告知参加人员保密要求，必要时签订保密承诺书。

对涉密文件、资料进行控制。例如，确定文件发放范围，做好发放登记；低空数据管理应有明显保密标识和会后回收标识；会议结束时，及时收回清点、登记。

### 3.9.5 国际合作

若涉及跨境低空合作，应审慎选择国际合作伙伴。在与国外企业或机构开展合作之前，应对合作伙伴及其关联单位进行背景调查和评估，包括是否是被制裁、被列入实体清单等管制清单的国家或主体，以及其在商业秘密保护方面的制度和措施、是否有过商业秘密泄露或侵权的不良记录等，避免因合作伙伴的原因致使自身面临被制裁、合作信息被泄露等风险。

## 3.10 侵权风险防控管理

聘请涉密岗位员工前，应开展必要的背景调查，全面了解其任职经历等关键信息，包括但不限于：是否已与原单位依法解除劳动合同、是否仍对原单位负有竞业限制或商业秘密保密义务、是否有过泄密行为等。同时，要求拟聘用员工以书面形式承诺所提供背景信息的真实性，并对虚假信息承担相应责任。必要时，可要求其额外签署不侵犯他人商业秘密的承诺书，从源头降低潜在法律风险。

若录用来自潜在竞争关系单位的员工，应采取针对性防范措施，包括但不限于：审核待录用员工与原单位之间的保密约定、义务、内容和范围，防范该员工在本单位内部公开或使用原单位的商业秘密；提醒待录用员工不应将原单位的商业秘密带入本单位进行使用或公开；定期对已入职员工从事业务内容进行审核，排除使用原单位商业秘密。

在与供应商、客户、技术合作伙伴等第三方开展合作时，应评估其知识产权状况和合规风险，重点核查是否存在侵犯第三方商业秘密或其他权利争议的情形。保密协议应明确商业秘密的权利归属、使用权限及保密责任，明确要求对方保证其提供的一切信息、技术方案和服务成果均不侵犯任何第三方权益，否则须承担由此引发的全部法律责任与经济赔偿。对拟

引进或合作开发的技术信息、数据等文件开展权属与授权状态审查，确保其来源合法、权属清晰，杜绝使用第三方未授权或权属存疑的信息。

商业秘密管理部门应定期或不定期会同相关业务部门对项目研发、生产经营等关键环节开展商业秘密侵权风险专项评估，识别可能接触第三方商业秘密的场景及各环节可能存在的商业秘密侵权风险，形成风险清单及应对预案。

### 3.11 应急管理

各创新主体应定期对商业秘密保护与管理情况进行检查和评估，并形成书面报告，检查内容应包括：

a)根据本单位在低空经济产业链条的位置，评估商业秘密保护制度的适宜性、实施情况等；

b)研发、管理、销售、生产、质控、财务、供应链等环节涉密人员的履职情况；

c)涉密人员的保密协议签署、权限管理及离职管控情况；

d)研发中心、数据中心、生产区域、试飞基地等涉密区域管理情况；

e)低空飞行器设计图纸、飞控算法、飞行测试数据、航线规划等商业秘密事项的定密、分级、变更、解密、销毁情况；

f)适航认证、空域审批等特殊环节商业秘密管理情况；

g)涉密文件资料、计算机的管理情况；

h)电子邮箱、聊天工具、设计软件、存储软件等工具软件使用商业秘密的情况；

i)涉密账户、电子信息、操作系统、办公软件的管理情况；

j)涉密载体、物品的管理情况等。

相关创新主体应建立商业秘密泄露或侵权应急机制及预案，明确责任相关方与处理程序，包括以下内容：

a)针对商业秘密泄露、侵权等紧急情况策划应急预案，并针对科研合作项目，建立商业秘密泄露及侵权风险前置预判流程；

b)对策划的预案和响应措施进行培训，引导员工对商业秘密可能泄露的异常状况保持警觉；

c)定期对策划的应急预案和响应措施进行测试或演练，引导员工对可能的商业秘密泄露迹象及时报告上级；

d)建立内外部举报机制，对举报侵犯商业秘密的相关行为给予奖励；

e)对于外部商业敏感信息，及时核实其合法来源；

f)对于合法获取的外部商业秘密，及时检查各使用环节是否符合相关法律及合同要求。

相关创新主体应对已发生的商业秘密泄露、侵权事件等紧急情况做出响应，包括但不限于以下内容：

a)启动应急预案，成立商业秘密维权处理小组，快速研判事件等级并分级响应，阻断泄露渠道；

b)对商业秘密泄露、侵权等紧急事件核查，确认事件发生的事实和过程；

c)分析商业秘密泄露或侵权原因，判断是否侵权，确定泄露信息是否满足商业秘密的构成要件；

d)调查涉事人员、责任人等；

e)评估泄露、侵权程度及其影响；

f)收集、固定相关证据；

g)及时采取相应措施确保全程跟进维权进展，保证维权活动顺利进行

并处置相应的应急事项。

相关创新主体应及时更新商业秘密清单，升级技术防护措施，开展案例复盘培训；增加特殊场景应对情形，针对员工跳槽泄密、黑客攻击泄密和供应商泄密等不同场景完善防护措施。

## 4 商业秘密的维权

### 4.1 维权途径的选择

对侵犯商业秘密的违法行为，低空经济产业相关创新主体应依法主张权利，要求停止侵权，消除影响，赔偿损失。商业秘密维权途径主要有四种，包括：

1.向市场监督管理部门投诉举报；

2.向人民法院提起民事诉讼；

3.向公安机关控告；

4.申请劳动仲裁或商事仲裁。

以下是不同维权途径的路径特点：[4]

| | 行政途径 | 民事途径 | 刑事途径 |
|---|---|---|---|
| 立案门槛 | 提供有违法行为的初步证据。 | 采用立案登记制，对立案进行形式审查。 | 经过公安机关审查后，认为确有犯罪事实、需要追究刑事责任的，才能决定予以立案。 |
| 证明标准 | 市场监管部门依法享有行政强制调查权，可以有效弥补权利人私力取证的不足。 | 权利人需自行明确商业秘密的内容，自行收集证据举证证明主张保护的信息构成商业秘密、侵权行为的具体表现、侵权损失数额，举证不能将承担不利的法律后果。有条件适用举证责任倒置。 | 虽然权利人仅需完成其享有商业秘密、被告人/被告单位实施了侵害商业秘密的犯罪行为、其遭受的经济损失达到刑法追诉金额的初步举证责任即可，但刑事诉讼要求证据确实、充分，需达到排除合理怀疑的严格证明标准。 |

[4] 来源于深圳市中级人民法院发布的《企业商业秘密管理与维权指引》4.4 维权途径的路径特点。

| | 行政途径 | 民事途径 | 刑事途径 |
|---|---|---|---|
| 赔偿范围 | 一般对行为人处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。 | 权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益、法定赔偿。行为人故意侵害商业秘密，情节严重的，权利人有可能获得高达五倍的惩罚性赔偿。 | 仅对被告人/被告单位定罪量刑，不处理权利人经济赔偿问题，权利人获偿范围有限，往往难以填平损失，更不包括惩罚性赔偿。 |
| 维权周期 | 取证查处快，维权周期短。 | 6-12 个月，可能因公告送达管辖权异议、申请追加当事人、延长举证期限，司法鉴定中止审理等事由被延长。 | 侦查期限 2-7 个月，审查起诉期限 1-2 个月，法院审理期限 3-6 个月。如需进行补充侦查、发现漏罪、查明被告人身份的情形前述期限将相应延长。 |

商业秘密维权案件中，如需进行商业秘密鉴定，可参考由中国知识产权研究会知识产权鉴定专业委员会公布的知识产权鉴定机构名录库，其官方信息发布渠道为 http://www.cnips.org.cn。

## 4.2 行政途径

### 4.2.1 投诉举报

相关创新主体商业秘密被他人不正当竞争行为侵犯的，可以向市区两级市场监督管理部门投诉举报，由市场监督管理部门进行认定查处后实施行政处罚。对市场监督管理部门作出的行政处罚决定不服的，可依法提起行政复议或行政诉讼。

### 4.2.2 管辖

举报由被举报行为发生地的县级以上市场监督管理部门处理，法律、行政法规、部门规章另有规定的，从其规定。向市场监督管理部门提出举

报的，应当通过市场监督管理部门公布的接收举报的互联网平台、电话、邮寄地址、窗口等渠道进行。深圳地区还可通过“深圳 12345”微信公众号，按照页面提示填写相关信息，上传请求书、相关证据等附件。

#### 4.2.3 投诉范围

投诉涉及的侵权行为指《中华人民共和国反不正当竞争法》第十条列举的侵犯商业秘密的行为：

a)以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；

b)披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

c)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；

d)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。

e)经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密；

f)第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

不属于侵犯商业秘密的行为：

a)通过自行开发研制取得的信息。研发记录应与主张商业秘密信息的内容相同或实质性相同；自行开发研制信息的完成时间，如早于他人相关权益的形成时间，通常可认定主张合法权益的抗辩理由成立；

b)通过反向工程获得信息。《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》第十四条规定，反向工程指通过技术手

段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。但是以不正当手段获取权利人的商业秘密后，又以反向工程为由主张未侵犯商业秘密的除外；

c)通过商业秘密权利人许可、转让而合法取得信息。许可或转让合同应当载明商业秘密的具体内容，可以对商业秘密载体中的内容进行总结、概括、提炼来形成商业秘密的具体内容；

d)通过分析、研究公开资料、信息、技术组合取得信息。该信息应当同时满足不为所属领域的相关人员普遍知悉和容易获得两个条件；

e)因商业秘密权利人自己的疏忽，造成商业秘密泄露使他人获得。以合法渠道、正当手段善意取得相关信息，不构成侵权；

f)通过其他合法渠道取得商业秘密。

#### 4.2.4 证据准备

权利人通过行政路径保护商业秘密时需要提交的证据材料主要包括以下几种：

1.请求保护的商业秘密权利主体资格。请求人应为该商业秘密的权利人，或者与权利人具有独占使用许可、排他使用许可关系的被许可人。普通使用许可合同的被许可人须经权利人书面授权。

2.请求保护的商业秘密应符合商业秘密的法定构成要件。包括该商业秘密的产生过程、载体、具体秘密点内容、商业价值、不为公众所知悉以及对其采取的具体保密措施等。

3.被举报人具有接触或实施侵犯该商业秘密行为的相关证明材料。

4.被举报人使用的技术信息和经营信息与投诉人请求保护的技术信息和经营信息具有一致性或相同性。

5.证明因该商业秘密被泄露造成的损失或侵权人的获利，以及因维权

产生的律师费、鉴定费、评估费等费用。

6.其他表明商业秘密被侵犯的证据。

#### 4.2.5 行政责任

根据《中华人民共和国反不正当竞争法》第二十六条，违反本法第十条规定侵犯商业秘密的，由市场监督管理部门责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

### 4.3 民事途径

#### 4.3.1 主体资格

提起侵害商业秘密纠纷的原告可以为技术秘密和经营秘密的开发者，或者受让人、继承人、权利义务的承继者等权利人，也可以为商业秘密的被许可人。具有下列情形之一的，被许可人具备原告诉讼主体资格：

1.商业秘密独占使用许可合同的被许可人可以单独作为原告提起诉讼；

2.排他使用许可合同的被许可人可以和权利人共同提起诉讼，或者在权利人不起诉的情况下自行提起诉讼；

3.普通使用许可合同的被许可人可以和权利人共同提起诉讼，或者经权利人书面授权单独提起诉讼。

#### 4.3.2 管辖

因侵害商业秘密提起的诉讼，由侵权行为地或者被告住所地人民法院管辖[5]。侵权行为地，包括侵权行为实施地、侵权结果发生地[6]。侵权结果

[5] 《中华人民共和国民事诉讼法》第二十九条规定，因侵权行为提起的诉讼，由侵权行为地或者被告住所地人民法院管辖。

[6] 最高人民法院关于适用《中华人民共和国民事诉讼法》的解释第二十四条规定，侵权行为地，包括侵权行为实施地、侵权结果发生地。

地应当理解为侵权行为直接产生结果的发生地，不能简单地以原告受到损害就认定原告住所地是侵权结果发生地。

深圳市中级人民法院知识产权法庭管辖深圳市辖区内第一审技术秘密纠纷民事案件以及 50 亿元以下超出基层法院管辖标的的经营秘密纠纷案件。对技术秘密纠纷民事一审判决不服的，向最高人民法院知识产权法庭提起上诉。深圳市各区法院审理各自辖区内标的额在 1000 万元以下的第一审经营秘密纠纷民事案件。

#### 4.3.3 维权材料

1.认定商业秘密的证据材料、认定侵权形成及结果的证据材料；

2.《民事起诉书》或《仲裁申请书》等，详细陈述商业秘密的有效存在、内容、价值，行为人违反劳动合同的约定、存在侵犯企业商业秘密的行为，并且企业的损失与行为之间存在因果关系。

#### 4.3.4 证据保全

在证据可能灭失或者以后难以取得的情况下，当事人可以在诉讼过程中向人民法院申请保全证据。人民法院也可以主动采取保全措施。当事人可以在起诉前申请证据保全，也可以在起诉后申请证据保全。申请证据保全的，应当在举证期限届满前向人民法院提交书面申请[7]。

商业秘密纠纷案件中申请证据保全的，应当在保全申请中明确商业秘密的具体内容，同时提供载有商业秘密的文档、计算机软件、产品、数据库等证据。

#### 4.3.5 行为保全

对于可能因当事人一方的行为或者其他原因，使判决难以执行或者造

[7] 《最高人民法院关于民事诉讼证据的若干规定》第二十五条规定，当事人或者利害关系人根据《中华人民共和国民事诉讼法》第八十四条的规定申请证据保全的，申请书应当载明需要保全的证据的基本情况、申请保全的理由以及采取何种保全措施等内容。当事人根据《中华人民共和国民事诉讼法》第八十四条第一款的规定申请证据保全的，应当在举证期限届满前向人民法院提出。法律、司法解释对诉前证据保全有规定的，依照其规定办理。

成当事人其他损害的案件，当事人可以向人民法院申请裁定责令其作出一定行为或者禁止其作出一定行为；当事人没有提出申请的，人民法院在必要时也可以裁定采取保全措施[8]。当事人可以在起诉前申请行为保全，也可以在起诉后申请行为保全。

诉前行为保全是利害关系人因情况紧急于诉前向人民法院申请禁止被申请人为一定行为的保全措施，以避免其合法权益受到难以弥补的损害。在侵害商业秘密纠纷案中，如果涉案秘密在诉讼前夕存在被进一步泄露的风险，对权利人造成难以弥补的损害，权利人可以及时向法院申请行为保全。

#### 4.3.6 民事责任

根据《中华人民共和国反不正当竞争法》第二十二条，因不正当竞争行为受到损害的经营者的赔偿数额，按照其因被侵权所受到的实际损失或者侵权人因侵权所获得的利益确定。经营者故意实施侵犯商业秘密行为，情节严重的，可以在按照上述方法确定数额的一倍以上五倍以下确定赔偿数额。赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。

#### 4.3.7 仲裁

劳动合同或保密协议中有约定仲裁条款，或者发生纠纷后双方就纠纷的解决达成仲裁协议的，应当按照约定向相关仲裁机构申请仲裁。劳动仲裁由劳动合同履行地或者用人单位所在地的劳动争议仲裁委员会管辖。其他商事仲裁则应由仲裁协议约定的仲裁机构管辖。商事仲裁实行“一裁终局”制度，裁决自作出之日起即与人民法院生效的法律文书具有同等法律效力，当事人持有仲裁裁决书可以向人民法院申请强制执行。

对于劳动者与用人单位之间的因竞业限制协议引发的纠纷，如果用人

[8] 《中华人民共和国民事诉讼法》第一百零三条规定，人民法院对于可能因当事人一方的行为或者其他原因，使判决难以执行或者造成当事人其他损害的案件，根据对方当事人的申请，可以裁定对其财产进行保全、责令其作出一定行为或者禁止其作出一定行为;当事人没有提出申请的，人民法院在必要时也可以裁定采取保全措施。

单位以违约为由主张权利，则属于劳动争议，应当通过劳动争议处理程序解决；如果用人单位以侵犯商业秘密为由主张权利，则属于不正当竞争纠纷，人民法院可以直接予以受理。[9]

### 4.4 刑事途径

#### 4.4.1 管辖

依据《中华人民共和国刑事诉讼法》第十九条至第二十八条的规定，侵犯商业秘密刑事案件的侦查由公安机关进行，具体由犯罪行为地、犯罪结果地和犯罪嫌疑人居住地的公安机关管辖。

#### 4.4.2 立案追诉标准

根据《最高人民检察院 公安部关于修改侵犯商业秘密刑事案件立案追诉标准的决定》，【侵犯商业秘密案（刑法第二百一十九条）】侵犯商业秘密，涉嫌下列情形之一的，应予立案追诉：

1.给商业秘密权利人造成损失数额在三十万元以上的；

2.因侵犯商业秘密违法所得数额在三十万元以上的；

3.直接导致商业秘密的权利人因重大经营困难而破产、倒闭的；

4.其他给商业秘密权利人造成重大损失的情形。

#### 4.4.3 控告材料

1.认定商业秘密的证据材料、认定侵权行为及结果的证据材料。

2.《刑事控告书》，详细陈述商业秘密的有效存在、内容、价值、侵权人的侵权行为和侵权行为所造成的损害后果，以及犯罪经过。

3.商业秘密被侵权符合刑事立案标准的证据。

---

[9] 来源于深圳市中级人民法院发布的《企业商业秘密管理与维权指引》4.2.2 仲裁。

### 4.4.4 刑事责任

《中华人民共和国刑法》第二百一十九条规定，有下列侵犯商业秘密行为之一[10]，情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金。

《中华人民共和国刑法》第二百一十九条之一规定，为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，处五年以下有期徒刑，并处或者单处罚金；情节严重的，处五年以上有期徒刑，并处罚金。

不仅如此，对法人犯罪也有适用双罚制的规定。单位侵犯他人商业秘密的，对单位判处罚金，并对其直接负责的主管人员和其他责任人员，同样依照上述规定处罚[11]。

### 4.4.5 刑事附带民事诉讼

被害人可以在侵犯商业秘密罪的刑事诉讼过程中提起附带民事赔偿诉讼。[12]

在侵犯商业秘密罪中，只有因侵犯商业秘密犯罪行为导致商业秘密已为公众所知悉的，才符合《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第一百七十五条中规定的“财物被犯罪分子毁坏”。除此之外，其他侵犯商业秘密的犯罪行为导致的权利人的损失，例如市场份额的减少、销售利润的下降等，均不属于刑事附带民事诉讼范畴，人民法院应当不予受理。

---

[10] 《中华人民共和国刑法》第二百一十九条规定，有下列侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或者单处罚金;情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：(一)以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；(二)披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；(三)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的。//明知前款所列行为，获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。//本条所称权利人，是指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。

[11] 《中华人民共和国刑法》第二百二十条规定，单位犯本节第二百一十三条至第二百一十九条之一规定之罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照本节各该条的规定处罚。

[12] 《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》第一百七十五条规定，被害人因人身权利受到犯罪侵犯或者财物被犯罪分子毁坏而遭受物质损失的，有权在刑事诉讼过程中提起附带民事诉讼；被害人死亡或者丧失行为能力的，其法定代理人、近亲属有权提起附带民事诉讼。因受到犯罪侵犯，提起附带民事诉讼或者单独提起民事诉讼要求赔偿精神损失的，人民法院一般不予受理。

## 5 侵犯商业秘密典型案例

### 5.1 研发人员将公司代码披露至互联网，为何构成商业秘密犯罪？

**案例名称：**深圳市南山区人民法院审结深圳某无人机企业内部员工侵害商业秘密纠纷案

**案情介绍：**深圳某无人机名企，其无人机广泛应用于航拍、遥感测绘、森林防火等领域，尖端产品农业植保无人机 1 小时可作业 150 亩。2017 年 9 月初，该公司漏洞举报邮箱收到海外邮件，称在互联网的 GitHub 代码分享社区上，发现有包含公司源代码等重要敏感信息的链接，该社区对全球用户可见，可能严重影响公司知识产权。经调查，泄露事件系公司 28 岁软件硕士阿辉所为。阿辉毕业于著名高校，负责编写农业无人机管理平台和农机喷洒系统代码，其在 GitHub 开设账号并建立“公有仓库”，通过计算机指令将含公司相关模块代码上传至该仓库，导致源代码泄露。

**法律依据及处罚：**经鉴定，泄露的代码具有非公知性、实用性，公司已采取合理保密措施，属于商业秘密；经评估，此次泄露给公司造成 116.4 万元经济损失。阿辉入职时曾签订《保密协议》，公司《员工信息安全守则》也明确技术细节为“最核心机密”，严禁泄露至外部可接触平台，但阿辉仍明知故犯。根据《中华人民共和国刑法》规定，违反权利人关于保守商业秘密的要求，披露其所掌握的商业秘密，造成严重后果，应当以侵犯商业秘密罪追究刑事责任。一审以侵犯商业秘密罪判决阿辉有期徒刑六个月，并处罚金 20 万元人民币。

### 5.2 如何证明技术信息是否属于非公知性信息？

**案例名称：**北京知识产权法院审结周某等 4 人侵犯某科技有限公司技术秘密案

**案情介绍：**某科技有限公司（简称某科技公司）主要从事电子产品硬件研发及销售业务。周某等 4 人原系某科技公司员工，离职后成立某北京科技有限公司（简称某北京科技公司）、某廊坊有限公司（简称某廊坊公司）。某科技公司主张周某等 4 人窃取了其型号为 ZD300-24S220N 模块电源电路板的电路布局及工艺要求等技术秘密（简称涉案技术信息），并提供给某北京科技公司和某廊坊公司使用，以及某北京科技公司和某廊坊公司明知涉案技术信息是某科技公司的商业秘密仍用于生产、销售与某科技公司完全相同的产品行为违反了 2017 年修订的《中华人民共和国反不正当竞争法》（简称 2017 年反不正当竞争法）第九条第一款、第二款的规定，故诉至北京知识产权法院，请求判令某北京科技公司、某廊坊公司立即停止侵犯商业秘密行为，连带赔偿经济损失 100 万元及合理支出 7716 元。

北京知识产权法院经审理认为，含有涉案技术信息的电源产品已经在被控侵权行为发生之前公开销售，所属领域技术人员很容易获得涉案技术信息，涉案技术信息已为公众所知悉，不符合 2017 年反不正当竞争法第九条第三款的规定，不构成商业秘密，故判决驳回某科技公司的诉讼请求。

某科技公司不服一审判决，向二审法院提起上诉。二审法院判决驳回上诉，维持原判。

**法律依据及处罚：**在被诉行为发生之前，某科技公司生产的承载涉案技术信息的产品已经公开销售，通过对公开销售的产品进行壳体拆卸、电路板去胶、对部分元件进行拆解和测量后，所属领域技术人员通过直接观察，很容易得到电路板上的电路布局、元件选择、连接关系和工艺要求等涉案技术信息，而去胶、拆解、测量所用到的仪器是恒温烙铁、数字电桥、数显卡尺、万用表等常规仪器，且具体的拆解测量过程较为简单，不需要

特殊的技艺或付出过高成本。同时，对于磁芯及骨架型号、绝缘胶带宽度、导线规格和绕线圈数、磁芯中心是否开气隙等技术信息，所属领域技术人员在简单拆解的基础上，结合行业一般知识即可获得。因此，某科技公司主张的涉案技术信息不符合商业秘密“不为公众所知悉”的法定要件，不构成 2017 年反不正当竞争法第九条第三款所保护的商业秘密。

### 5.3 单一客户名单和信息能否作为商业秘密保护？

**案例名称：**北京市海淀区人民法院审结陈某、石某等侵犯某公司客户名单等经营信息商业秘密纠纷案

**案情介绍：**2012 年 7 月，陈某、石某入职北京万岩通软件有限公司（下称万岩通公司），签署了包括《保密协议》等一系列具有保密性质的协议。二人在职期间受万岩通公司指派，参与了与中石油管道分公司（下称管道公司）项目合作，涉及移动应用平台项目。2014 年 5 月 7 日，陈某配偶李某与石某（后变更为石某之母韩某）作为自然人股东成立北京恰行者科技有限公司（下称恰行者公司）。2014 年 6 月，陈某、石某自万岩通公司离职。后，陈某、石某以恰行者公司名义与管道公司开展合作，2014 年 12 月，恰行者公司与管道公司签订《移动应用平台技术服务合同》。2015 年 11 月，管道公司信息中心出具《移动应用平台项目任务书》，邀请恰行者公司作为单一来源方谈判采购，恰行者公司报价为 235 万元。另，恰行者公司与管道公司合作期间，其接触的管道公司项目负责人有曹某、安某、张某等人，上述人员同为陈某、石某在万岩通公司任职期间接触到的管道公司相关项目人员。

万岩通公司主张恰行者公司、陈某、石某侵犯其商业秘密即客户名单，其内容包括管道公司客户交易习惯、需求、价格承受能力、项目负责人的

性格特点、联系方式、地址以及万岩通公司与其形成的稳定交易关系，故起诉至北京市海淀区人民法院（简称海淀法院），要求三被告恰行者公司、陈某、石某停止侵害原告商业秘密的行为，公开赔礼道歉、消除影响，共同赔偿原告经济损失 50 万元及合理费用 2 万元，并承担本案诉讼费用。

**法律依据及处罚：**海淀法院经审理认为，原告和被告恰行者公司的经营范围、服务对象均存在重合，已构成竞争关系。原告主张应作为商业秘密保护的涉案客户名单，系与其保持长期稳定合作关系的特定客户管道公司，包括客户交易习惯、性格特点、价格承受能力、交易偏好等信息，具有秘密性、价值性和保密性，属于商业秘密。被告陈某、石某利用在原告任职的职务便利获取涉案商业秘密，在离职后通过关联关系人恰行者公司，与原告涉案特定客户签订相关技术服务合同，其行为构成反不正当竞争法第十条第一、二款规定的侵犯商业秘密。据此判决三被告停止侵害原告涉案商业秘密的行为、共同赔偿原告经济损失 20 万元、律师费 1.6 万元，并消除影响。宣判后，三被告不服一审判决，提起上诉。北京知识产权法院判决驳回上诉，维持原判。

### 5.4 从多份不同文件提炼出的技术信息可否作为技术秘密保护？

**案例名称：**最高人民法院审结程某卓、爱兴公司与博阳公司侵害技术秘密纠纷案

**案情介绍：**在上诉人程某卓、成都爱兴生物科技有限公司（以下简称爱兴公司）与被上诉人科美博阳诊断技术（上海）有限公司（以下简称博阳公司）侵害技术秘密纠纷案中，博阳公司认为，其研发的用于临床免疫诊断领域的“光激化学发光分析系统通用液（LiCA）”相关技术信息构成不为公众知悉的技术秘密，系从《LiCA 通用液生产工艺规程》《发光微

粒质量标准》《感光试剂缓冲液配制记录》等多份内部技术文件中提炼、总结而成的技术信息组合。程某卓原为博阳公司的核心技术开发人员，系统掌握了上述技术秘密，离职后进入爱兴公司并将其掌握的上述技术秘密擅自披露给爱兴公司，爱兴公司在生产、销售的体外诊断试剂盒产品中直接使用了其技术秘密，故向上海知识产权法院（以下简称一审法院）提起诉讼。

一审法院认为，博阳公司主张的技术信息不为公众所知悉、具有商业价值并且对该技术信息采取了合理保密措施，构成技术秘密，程某卓、爱兴公司实施了侵害技术秘密的行为，故判决程某卓、爱兴公司停止侵害并共同赔偿经济损失 100 万元、维权合理开支 30 万元。程某卓、爱兴公司不服，向最高人民法院提起上诉，主张博阳公司的工艺规程等文件仅反映了其主张的技术秘密方案中的零散、个别要素，没有体现完整的技术方案，涉案技术秘密中技术方案的完整内容与其提交的工艺规程等载体文件不具有对应性，不能证明涉案技术秘密系其自行研发。最高人民法院于 2022 年 12 月 14 日判决驳回上诉，维持原判。

**法律依据及处罚：**最高人民法院二审认为，技术秘密通常以图纸、工艺规程、质量标准、操作指南、实验数据的形式来体现，权利人为证明其技术秘密的存在及其内容，通常会在体现上述技术秘密的载体文件基础上，总结、概括、提炼其需要保护的技术信息，其技术秘密既可以是技术方案，也可以是构成技术方案的部分技术信息。

本案中，博阳公司主张的技术秘密为 8 个技术方案，每一技术方案包括若干技术信息，在后技术方案对在前技术方案的技术信息作出进一步限定或增加，从而形成层层递进的技术方案。涉案技术秘密中的微粒 CV 值、粒径等技术信息在博阳公司的技术文件中均有对应记载。

博阳公司根据其技术文件，并结合本领域的现有技术、公知常识的合理总结与提炼，能够证明博阳公司实际拥有并掌握上述技术方案，程某卓、爱兴公司关于涉案技术秘密的相应信息没有载体予以对应、不能证明博阳公司为涉案技术秘密权利人的主张不能成立。

### 5.5 通过发放员工手册约定的竞业限制是否有效？

**案例名称：**北京市朝阳区人民法院审结郭某诉资管北京分公司劳动争议案——竞业限制义务与保密义务的辨析与认定

**案情介绍：**2018 年 4 月 13 日，郭某入职企业管理公司，担任高级顾问。2018 年 9 月 1 日，资管北京分公司、企业管理公司及郭某签订三方协议，约定：2018 年 9 月 1 日起，郭某的用人单位由企业管理公司变更为资管北京分公司。郭某的月基本工资标准为 15000 元。劳动合同书约定“根据岗位及工作性质，郭某同意在资管北京分公司需要的情况下与其签订竞业限制协议”，“郭某违反与资管北京分公司签订的服务期约定或竞业禁止约定的，应按照相关约定向该公司支付违约金”。2019 年 3 月 13 日，郭某因个人原因离职，双方劳动关系解除。资管北京分公司主张，根据《员工手册》第 5.9 条规定，离职后六个月为竞业限制期限：“……不论因何种原因从公司离职，离职后六个月内不得到与公司有竞争关系的单位就职；不论因何种原因从公司离职，离职后六个月内不得自办与公司有竞争关系的企业或从事与公司商业秘密有关的职务及自办企业……”郭某离职后，入职与其公司具有竞争关系的商务咨询公司，同样从事人才服务，已违反竞业限制义务，应按规定支付基本工资的十倍作为违约金。郭某不予认可，主张双方未达成过竞业限制的协议，其不受竞业限制的约束。

**法律依据及处罚：**北京市朝阳区人民法院于 2020 年 8 月 19 日作出

（2020）京 0105 民初 21792 号民事判决：一、原告无需支付被告竞业限制违约金 150000 元。二、案件受理费 5 元，由被告负担。宣判后，原被告均未上诉。法院生效裁判认为，本案争议焦点为《员工手册》是否可以作为郭某承担竞业限制义务的依据。我国劳动合同法规定，对负有保密义务的劳动者，用人单位可以在劳动合同或者保密协议中与劳动者约定竞业限制条款，并约定在解除或者终止劳动合同后，在竞业限制期限内按月给予劳动者经济补偿。因此，竞业限制义务的承担需以用人单位与劳动者存在竞业限制约定为前提。该种约定可以在劳动合同中设置相关条款，也可以单独签署保密协议或竞业限制协议予以明确。竞业限制条款的本质是契约，需在用人单位与劳动者平等协商的基础上，形成双方真实意思表示的合意。

而《员工手册》是用人单位规章制度的一种，是用人单位行使用工管理权的方式之一，通常在劳动者入职之前已经制定。竞业限制的内容应由双方平等协商确定，不应通过规制制度来事先确定。用人单位通过《员工手册》要求劳动者承担竞业限制义务有可能导致竞业限制协议对全体员工统一适用，不当扩大竞业限制的适用范围，影响无关人员的择业自由。因此，用人单位在《员工手册》中规定竞业限制义务的，对劳动者不具有法律约束力。

本案中，资管北京分公司与郭某签订的劳动合同书中亦约定若需承担竞业限制义务需另行签订竞业限制协议，现资管北京分公司依据《员工手册》的规定，要求郭某承担竞业限制违约金，缺乏法律依据，故对郭某要求无需支付资管北京分公司竞业限制违约金 150000 元的诉讼请求，法院予以支持。

### 5.6 第三人使用他人非法获取的商业秘密是否构成商业秘密侵权？

**案例名称：**芜湖市市场监管局查处安徽某航空公司侵犯商业秘密案

**案情介绍：**安徽某航空科技有限公司（下称“权利人公司”）以螺旋桨及动力系统配件的研发、制造与销售为核心业务，其自主研发的复合材料螺旋桨固化成型工艺是公司生存发展的重要支柱，具备显著商业价值。同时公司建立了严格的保密体系，针对包括复合材料螺旋桨固化成型工艺在内的商业秘密进行严格保护。此外经司法鉴定机构确认，该工艺属于不为公众所知悉的技术信息，构成受法律保护的商业秘密。

权利人公司的两名前员工翟某与袁某任职于涉及该商业秘密的关键岗位，在入职时均签署了《保密协议》，需遵守公司保密管理规定。两人从权利人公司离职后，先后加入安徽云翔航空科技有限公司（后更名为云翔航空科技（芜湖）有限公司，下称“云翔公司”）。值得注意的是，云翔公司的两任法定代表人，分别与翟某、袁某存在亲属关系，这一特殊关联在认定云翔公司“应知”但仍使用负有保密义务的翟某、袁某所提供的商业秘密的过程中，起到了重要的参考作用。

经司法鉴定机构进一步鉴定，安徽云翔航空科技有限公司用于生产的技术，与权利人公司研发的复合材料螺旋桨固化成型工艺技术实质相同。据此，芜湖市市场监管局认定云翔公司作为第三人，在明知或应知相关技术为他人商业秘密的情况下，仍使用了对权利人公司负有保密义务的前员工所掌握的工艺技术，其行为已构成违法行为。

**法律依据及处罚：**云翔公司的行为违反了《中华人民共和国反不正当竞争法》第九条第三款的规定，即第三人明知或应知商业秘密来源非法仍予以使用的情形。依据该法第二十一条，芜湖市市场监管局责令云翔公司停止违法行为，并处以 37 万元罚款，接近法定罚款上限（50 万元）。此外，市场监管部门还对涉事员工翟某、袁某立案调查，可能进一步追究其

民事或刑事责任。

### 5.7 侵犯客户名单等经营信息是否构成商业秘密侵权？

**案例名称：**咸宁市中级人民法院审结刘某、姚某、雷某等侵犯某公司经营信息案

**案情介绍：**甲公司长期从事无人机研发、生产与销售，其掌握的客户信息包含客户姓名、公司名称、联系方式、具体需求及交易习惯等核心内容，具有较高商业价值且不易被外界知悉。同时甲公司建立了严密的保密体系，包括具有保密条款的劳动合同、《采购岗位保密协议书》以及规定需使用工作手机防止客户信息泄露等保密措施。

刘某、姚某、雷某均为甲公司的前员工，其中刘某担任网络运营职务，姚某、雷某担任外贸业务员。具体地，姚某、雷某与甲公司签订了包含保密条款的劳动合同、《采购岗位保密协议书》、《工作手机领用合同》等协议以防止客户信息泄露；刘某虽未与甲公司书面签订劳动合同，但其作为甲公司的网络运营人员，实际知晓公司保密要求。两人均处于接触甲公司的商业秘密的岗位，且对该商业秘密负有保密义务。

后来，姚某、雷某通过其丈夫名义与刘某共同成立乙公司，主要开展无人机配件销售业务，与甲公司构成竞争关系。自 2022 年 10 月起，姚某陆续撮合甲公司的部分客户与乙公司达成交易，期间刘某和雷某对相关交易起到积极的推动作用。2022 年 12 月，姚某将甲公司客户信息转移至个人微信，并向乙公司、刘某以及雷某披露，侵犯了甲公司的商业秘密。据统计，共有 12 家原甲公司客户与乙公司交易，乙公司获利共计人民币达 87 万元及 4.2 万美元。

甲公司发现刘某等人涉嫌侵犯其商业秘密的行为后，对刘某、姚某、

雷某作出停职处理，并向公安机关报案。同时，甲公司向法院提起诉讼，要求判令侵权方停止侵权行为，并赔偿经济损失。一审法院判决乙公司及刘某、姚某、雷某的行为构成共同侵权，立即停止披露、使用涉案 67 家客户信息，并连带赔偿甲公司经济损失 50 万元。四被告均不服，并提出上诉。

**法律依据及处罚：**湖北省咸宁市中级人民法院认为，本案中甲公司主张的客户信息符合《中华人民共和国反不正当竞争法》中商业秘密的“三要素”的定义，应被认定为商业秘密。其中，刘某虽然未与甲公司签订规定有保密措施的相关协议、合同，是因其所在岗位不涉及甲公司客户信息，但其实质却与姚某、雷某共同串通披露、使用甲公司的客户信息，证明其明知并认可甲公司采取相应保密措施，也因此应认定甲公司已经就案涉客户信息采取相应保密措施。

一审法院判决乙公司及刘某、姚某、雷某的行为构成共同侵权，违反《中华人民共和国反不正当竞争法》第九条关于禁止侵犯商业秘密的规定。法院判决侵权方立即停止披露、使用涉案 67 家客户信息，并连带赔偿甲公司经济损失 50 万元。

### 5.8“窃而未用”侵犯商业秘密吗？

**案例名称：**福州市鼓楼法院审结苏某侵犯 T 游戏公司商业秘密纠纷案

**案情介绍：**苏某于 2022 年 10 月 20 日入职 T 游戏公司，担任中级系统策划，与公司签有保密协议。其中约定若苏某违反保密义务的，应当无条件向公司支付相当于员工本人离职前最后一个月的月工资的 3 倍金额以承担违约责任，若对公司造成实际经济损失还应承担相关费用。2023

年 3 月 9 日，苏某计划离职，并对 T 游戏公司的八份重要文件进行了复制、查看、修改公开范围和访问权限等操作。T 游戏公司发现后立即电话通知苏某至公司当面销毁全部拷贝资料，苏某回复“只是蛮拷一下而已”并同意回公司处理。2023 年 3 月 14 日，苏某自述已删除相关文件，并与 A 公司签订了《劳动合同解除协议书》。2023 年 8 月 2 日，T 游戏公司将苏某诉至法院。

T 游戏公司认为虽然苏某自述已将拷贝的文件资料销毁，但客观上是否销毁、是否仍有保留，T 游戏公司不得而知，苏某的行为严重破坏了 T 游戏公司对于商业秘密的完整控制权，使 T 游戏公司商业秘密信息处于不安全和不稳定状态，且严重违反双方协议，据此苏某应当依据《劳动合同解除协议书》的约定向 T 游戏公司支付违约金 4.5 万元（按其最后一个月工资的 3 倍计算，即 1.5 万元/月*3 倍）。

**法律依据及处罚：**福州市鼓楼法院审理认为，T 游戏公司提交了案涉文件，内容包括了每日在线人数、平均用户充值金额、平均付费用户充值金额、付费率、考核指标等经营信息，不为公众所知悉，能够为权利人带来商业利益，且 T 游戏公司采取了约定保密义务、设置电子文件权限等相应的保密措施，构成商业秘密。《反不正当竞争法》第九条第一款第一项规定：“经营者不得实施下列侵犯商业秘密的行为：（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密”，法院认为，本案中，苏某系 T 游戏公司的系统策划，在离职时已经知晓不得复制、保留或带离 T 游戏公司，但其通过不正当手段，非法获取了案涉商业秘密，侵犯了 T 游戏公司享有的商业秘密，依法应承担赔偿损失的责任。

在侵权赔偿数额方面，《反不正当竞争法》第十七条并未禁止被侵权

人与侵权人就侵权责任的方式、侵权赔偿数额等预先作出约定。这种约定的法律属性，可认定为双方就未来发生侵权时权利人因被侵权所受到的损失或者侵权人因侵权所获得的利益，预先达成的一种简便的计算和确定方法。本案中，双方已就非法获取商业秘密的行为预先约定了赔偿数额，未违反法律规定，且未明显超出合理范围，故鼓楼法院参照前述约定，酌定苏某赔偿 T 游戏公司经济损失及合理费用共计 4.5 万元。

### 5.9 因侵权造成的权利人销售利润损失难以计算时如何认定？

**案例名称：**最高人民法院审结王龙集团公司及其法定代表人侵犯技术秘密案件

**案情介绍：**嘉兴市中华化工有限责任公司（以下简称嘉兴中华化工公司）、上海欣晨新技术有限公司拥有使用乙醛酸法制备香兰素工艺的技术秘密。嘉兴中华化工公司基于该工艺一跃成为全球最大的香兰素制造商，占全球市场约 60%的份额。王龙集团有限公司（以下简称王龙集团公司）及其法定代表人等通过嘉兴中华化工公司香兰素车间副主任非法获取了该技术秘密，并使用该技术秘密工艺大规模生产香兰素产品，导致香兰素产品价格下滑、嘉兴中华化工公司的市场份额缩减。嘉兴中华化工公司等遂诉至法院。一审法院认定王龙集团公司等构成侵害部分技术秘密，判决其停止侵害、赔偿经济损失 350 万元，同时作出行为保全裁定，责令立即停止侵害涉案技术秘密。一审判决后，王龙集团公司继续实施侵权行为。双方当事人提起上诉。

**法律依据及处罚：**最高人民法院二审认为，王龙集团公司系其法定代表人为侵权而设立的企业，且其法定代表人积极参与侵权行为的实施，故王龙集团公司与其法定代表人构成共同侵害全部技术秘密，应当承担连带

赔偿责任。根据权利人提供的经济损失数据，综合考虑涉案技术秘密商业价值大、侵权情节恶劣、被告拒不执行人民法院行为保全裁定等因素，改判王龙集团公司及其法定代表人等连带赔偿 1.59 亿元。由于王龙集团公司、王龙科技公司及喜孚狮王龙公司在本案中拒不提交与侵权行为有关的账簿和资料，二审法院无法直接依据其实际销售数据计算销售利润。考虑到嘉兴中华化工公司香兰素产品的销售价格及销售利润率可以作为确定王龙集团公司、王龙科技公司及喜孚狮王龙公司相关销售价格和销售利润率的参考，为严厉惩处恶意侵害技术秘密的行为，充分保护技术秘密权利人的合法利益，二审法院决定以嘉兴中华化工公司香兰素产品 2011-2017 年期间的销售利润率来计算本案损害赔偿数额，即以 2011-2017 年期间王龙集团公司、王龙科技公司及喜孚狮王龙公司生产和销售的香兰素产量乘以嘉兴中华化工公司香兰素产品的销售价格及销售利润率计算赔偿数额。

# 6 深圳市商业秘密保护公共服务资源

## 6.1 商业秘密管理体系建设辅导服务

2022 年 4 月 25 日，深圳市市场监督管理局正式发布《企业商业秘密管理规范》深圳市地方标准。该标准于 2021 年 4 月批准立项，并由广东深圳（南山）商业秘密保护基地牵头，联合华为、腾讯、比亚迪、迈瑞等知名企业、律所和科研院所，在总结梳理知名企业商业秘密管理经验的基础上，结合企业发展各阶段商业秘密保护需求，完成标准的制定。

为推动《企业商业秘密管理规范》深圳市地方标准的实施应用，经企业自愿报名，基地于 2021-2025 年共完成了 253 家不同领域、规模的试点企业标准落地辅导工作，在保护企业商业秘密、解决侵权取证困难等方面都取得了显著成效。

现《企业商业秘密管理规范》深圳市地方标准推广及企业商业秘密管理体系建设辅导工作仍在持续进行中，有意愿的企业可登录网址 https://amr.sz.gov.cn/xxgk/qt/ztlm/symmbh/tzgg/content/post_12211775.html，查看《深圳市市场监督管理局关于征集<企业商业秘密管理规范>深圳市地方标准第五批试点企业的通告》，下载填写附件《企业商业秘密管理规范》深圳市地方标准试点企业申请书，发送至邮箱 nsippc@szns.gov.cn。基地将在 5 个工作日内审查申请书，并电话通知企业，后续将采取专题辅导会、专家“一对一”问诊等方式辅导企业建立商业秘密管理体系。

## 6.2 商业秘密管理风险在线“体检”服务

商业秘密管理风险在线“体检”，是深圳市市场监管局联合深信服科技股份有限公司推出的一项服务举措。该项服务基于深信服科技股份有限公司的可拓展数据防泄密技术，可聚焦事前、事中、事后全流程，对企业内部的商业秘密数据流动情况进行智能化检测、预警、溯源，以实现识别泄密风险、保护商业秘密的目标。体检时长为 30 天，服务全程免费。

深圳市范围内有意愿参加商业秘密管理风险在线“体检”的企业，可扫描下方二维码填写相关信息，提交“体检”申请，根据自身情况自主选择两种不同的方式进行“体检”。

（一）“体检”服务方式

方式一：具备技术能力的企业，可选择“自助注册使用”方式，深圳市市场监管局收到“体检”申请后，将发送《商业秘密管理风险在线“体检”服务产品激活及使用手册》供企业参照。

方式二：不具备技术能力的企业，可选择“IT 助手辅助”方式，深圳市市场监管局收到“体检”申请后，将安排技术人员与企业进行联系，通过在线指导或上门服务的方式帮助企业安装“体检”工具。

（二）“体检”服务申请入口

### 6.3 涉外商业秘密保护“一对一”服务

2023 年 6 月 28 日，广东省市场监管局和深圳市市场监管局合力共建的黄金内湾涉外商业秘密保护基地正式揭牌成立。该基地以深圳知识产权保护中心为依托，围绕企业“走出去”的实际需要，聚焦服务保障、宣传引导、实务研究等环节，建立海外商业秘密纠纷监测与服务机制，增强企业防范应对海外商业秘密风险意识，提升商业秘密保护服务高水平对外开放的能力，护航黄金内湾各类创新主体公平参与国际竞争。

**一、申请条件**

申请人：黄金内湾地区合法注册的企事业单位、社会团体等主体。

申请费用：免费

**二、服务内容**

黄金内湾涉外商业秘密保护基地服务内容包括申请人在中国境外发生的如下商业秘密纠纷的应对指导咨询：

1.商业秘密侵权纠纷；

2.商业秘密相关贸易调查纠纷；

3.商业秘密相关让与/许可纠纷；

4.商业秘密合规管理；

5.其他商业秘密纠纷。

**三、申请流程**

申请材料、提交方式及办理流程参照海外知识产权纠纷应对指导深圳分中心纠纷应对指导规程

http://www.sziprs.org.cn/szipr/hwwq/sadsda/content/post_648065.html