# AIGC 企业商业秘密保护指引

北京市市场监督管理局发布

2026 年【 】月

# 前言

为深入贯彻落实北京市加快建设具有全球影响力的人工智能创新策源地、推动大模型技术创新突破与深度赋能千行百业的决策部署，全面强化本市 AIGC 企业商业秘密保护能力，筑牢技术创新与产业安全屏障，促进 AIGC 行业高质量发展，北京市市场监督管理局结合北京市 AIGC 企业发展实际，组织编制了本指引。

当前，生成式人工智能技术迭代迅猛、应用场景持续拓展，已成为数字经济创新发展的重要引擎。AIGC 企业在算法架构、模型训练、数据治理、核心代码、应用方案等方面投入巨大研发资源，其关键技术信息与核心经营信息构成企业核心竞争力，是商业秘密保护的关键对象。伴随行业高速发展，AIGC 企业泄密风险日益突出，侵权形态更趋隐蔽复杂，亟须构建完善的商业秘密保护体系。

本指引立足 AIGC 行业技术特性与产业实践，系统梳理商业秘密保护范围、核心秘密点及典型泄密风险，从 AIGC 行业商业秘密保护范围与秘密点的界定、内部管理体系的构建、外部保护途径及其衔接等关键环节入手构建完整保护框架，为 AIGC 企业提供系统性、针对性、可落地的保护指引，助力企业提升风险防范能力，保障本市 AIGC 行业持续健康发展。

本指引仅对北京市 AIGC 企业商业秘密保护提供一般性指引，不具有强制性。法律法规另有专门规定的，从其规定。

起草单位：

主要起草人：

# 目 录

# 第一章 概述

## 1.1 制定目的和法律依据

为全面提升本市AIGC企业商业秘密保护意识与全流程防护能力，有效防范模型、算法、数据、源代码等核心信息泄密风险，维护市场公平竞争秩序，激发企业创新活力，护航AIGC行业高质量发展，依据《中华人民共和国反不正当竞争法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国劳动合同法》《生成式人工智能服务管理暂行办法》《商业秘密保护规定》等法律法规规定，制定本指引。

## 1.2AIGC企业及业务范围

目前对于人工智能生成内容（Artificial Intelligence Generated Content，AIGC）这一概念的界定，尚无统一规范的定义。国内产学研各界对AIGC的理解是“继专业生成内容（Professional Generated Content，简称“PGC”）和用户生成内容（User Generated Content，简称“UGC”）之后，利用人工智能技术自动生成内容的新型生产方式”。[1]

本指引所称AIGC企业，是指在中国境内依法设立，从事AIGC技术研发、模型训练与微调、数据处理、产品开发、服务运营、技术服务及相关生态合作的企业、科研机构及其他经营主体。结合产业链分工，AIGC企业业务范围主要包括模型研发、工具服务、内容制作等。

（1）模型研发业务：从事生成式人工智能基础模型、垂类模型、多模态模型的算法研究、训练、微调、优化、推理与部署，开展底层框架、算力架构、训练策略及模型安全技术研发。

[1] 中国信息通信研究院和京东探索研究院《人工智能生成内容（AIGC）白皮书（2022年）》，第4页。

（2）工具服务业务：基于AIGC模型开发应用软件、SaaS平台、API接口、插件工具及行业解决方案，提供技术赋能、场景化部署与产品化服务。

（3）内容制作业务：运用AIGC技术开展文本、图像、音频、视频、虚拟形象等内容生成、编辑、合成、版权运营、IP开发与内容商业化运营。

1.3 其他术语及定义

（1）AIGC企业商业秘密：指AIGC企业在研发、训练、部署、运营、合作等过程中形成，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。

（2）定密：指企业按照规定，将符合条件的信息确定为商业秘密并进行分类、分级、标识、登记的管理行为。

（3）泄密：指违反保密义务或保密措施，非法获取、披露、使用、允许他人使用AIGC商业秘密的行为。

（4）涉密载体：指记载、存储、处理、传输AIGC商业秘密的各类介质，包括服务器与训练集群、数据库与向量数据库、代码仓库与制品库、模型仓库与模型注册中心、对象存储空间、容器镜像、训练检查点与中间产物、计算机、移动存储设备、云平台、纸质文件、电子文档等。

（5）涉密人员：指因工作需要接触、知悉、管理、掌握AIGC商业秘密的员工、研发人员、运维人员、管理人员、外包人员、合作方人员等。

（6）涉密区域：指用于研发、训练、存储、处理、保管AIGC商业秘密的物理场所与逻辑空间。物理涉密区域包括实验室、机房、数据中心、档案室、涉密办公区等；逻辑涉密区域包括模型训练与推理环境、代码仓库、模型仓库、数据湖与向量数据库、持续集成与交付流水线等。

# 第二章 AIGC 企业商业秘密保护范围与秘密点

## 2.1 商业秘密的概念及特征

根据《中华人民共和国反不正当竞争法》第十条第四款，商业秘密是不为公众所知悉，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。商业秘密具有秘密性、保密性和价值性三大特征。

### 2.1.1 秘密性

商业秘密的秘密性，是指在涉嫌侵犯商业秘密的行为发生时，有关商业信息不为其所属领域的相关人员普遍知悉和容易获得。将为公众所知悉的有关商业信息进行整理、改进、加工后形成新信息，不为所属领域的相关人员普遍知悉和容易获得的，具备秘密性。[2]

### 2.1.2 保密性

商业秘密的保密性，是指权利人为防止商业秘密泄露，采取与商业秘密及其载体的性质、商业秘密的商业价值等因素相适应的合理保密措施。[3]应当根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，认定权利人是否采取了相应保密措施。[4]

### 2.1.3 价值性

商业秘密的价值性，是指商业信息具有现实的或者潜在的价值，能为权利人带来资产增加、营业收入或者利润增长、用户数量增长、成本费用降低、研发时

[2] 《商业秘密保护规定》第六条。
[3] 《商业秘密保护规定》第九条。
[4] 《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》第五条。

间缩短、交易机会增加、商业信誉或者商品声誉提升等商业利益或者竞争优势。生产经营活动中形成的阶段性成果或者失败的实验数据、技术方案等信息，符合前述规定的，具备价值性。[5]

### 2.2 AIGC 企业商业秘密保护范围

商业秘密包括技术信息、经营信息等商业信息。

#### 2.2.1 技术信息保护范围

技术信息是指与技术有关的结构、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、数据、算法、代码、计算机程序及其有关文档等信息。[6]

AIGC 企业的技术信息是指在模型研发、算法开发、数据处理、工程化部署、内容生成、系统集成、评测与安全对齐等活动中形成的技术信息，本节所列各项是指企业在公知技术范式基础上形成的自研改造方案、具体实现细节及经验性取值，不包括已公开的技术范式、开源算法与通用架构本身。

（1）模型与算法类技术信息：模型结构与架构设计、预训练与微调机制、对齐与强化学习方法（RLHF/DPO 等）、模型权重及参数文件（含基础模型、LoRA、Adapter、ControlNet、微调 delta 权重等；其中基于开源底座训练所得的，指微调增量部分及其与底座的挂载配置）、模型压缩与优化方法（蒸馏、量化、剪枝等）、推理与解码策略、生成算法（含扩散、自回归、流匹配等）、跨模态映射与对齐逻辑、Agent 与多智能体协同机制、性能增强与加速技术等。

（2）数据与语料类技术信息：训练数据集、测试与评测数据集、人类偏好

---

[5] 《商业秘密保护规定》第七条。

[6] 《商业秘密保护规定》第五条第二款，《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》第五条第一款。

与反馈数据、合成数据及其生成方案、标注规则与标签体系、数据清洗与有害内容过滤方法、数据增强方法、向量化与嵌入（embedding）方案、数据集结构与切片（chunking）策略、语料库与知识库体系、知识图谱与知识映射关系等。

（3）代码与工程类技术信息：核心程序与源代码（含目标代码）、自研框架与中间件、API 接口协议与 SDK、模型服务化（Serving）与推理框架、算力调度与 GPU 资源管理方案、任务调度引擎、工作流编排文件（如 workflow.json、YAML 等）、兼容适配与多平台移植方案、部署架构与运维方案、安全防护与内容过滤的工程实现等。

（4）内容生成类技术信息：文本、图像、音频、视频、3D 等多模态内容生成的技术实现方案，包括但不限于：智能剪辑与后期处理、画质修复与超分、人物/角色/IP 一致性控制、风格迁移与个性化定制、长文本与长视频的上下文管理、提示词工程方案（系统提示词、模板库、负向词库、Few-shot 示例集等）、交互意图理解与多轮对话管理、内容质检与自动评测、安全对齐与有害内容拦截等。

（5）研发过程类技术信息：尚未公开的技术方案与技术路线图、实验数据与训练日志、失败实验与调优经验记录、测试与评测结果、版本迭代与变更记录、设计文档（含模型卡、数据卡、架构设计书等）、研发工具链与中间产物、研发计划与待研课题等。

### 2.2.2 经营信息保护范围

经营信息是指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。其中，客户信息包括客户的名称（姓名）、

地址、联系方式以及交易习惯、意向、内容等信息。[7]

AIGC 企业的经营信息是指在生产运营、商务合作、项目管理、资源调度、成本定价、客户服务、商业化落地等活动中形成的经营信息，主要包括：

（1）产品与规划类经营信息：未公开产品规划、功能设计、服务模式、迭代路线、商业化策略等。

（2）客户与商务类经营信息：客户信息、需求特征、合作方案、招投标信息、渠道资源、供应商信息、商务条款等。

（3）成本与定价类经营信息：成本核算体系、报价规则、定价策略、毛利率、成本测算方法、计价标准等。

（4）运营与调度类经营信息：生产效率模型、工期预测、资源调度、排期策略、风险预警、质量管控、流程规范等。

（5）项目与数据类经营信息：历史项目数据、产能数据、客户标签库、案例库、行业基准数据、运营分析结果等。

### 2.3 AIGC 企业商业秘密秘密点

商业秘密的秘密点是当事人主张的商业秘密信息的具体内容，[8]结合 AIGC 上游技术研发、中游工具服务、下游内容制作全产业链业务特点，按照“通用共性秘密点 + 产业链环节专属秘密点”体系化梳理如下：

#### 2.3.1 通用秘密点

（1）模型：模型架构（含网络结构设计、模块组合方式、层级拓扑关系等）、模型优化方法（含蒸馏、剪枝、量化、稀疏化等压缩与加速方案）、模型训练方

[7] 《商业秘密保护规定》第五条第三款，《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》第一条第二款。

[8] 《商业秘密鉴定规范》第三条 3.4。

法（含预训练策略、监督微调 SFT、基于人类反馈的强化学习 RLHF/DPO、持续学习与增量训练方案等）；

（2）数据：既包括特定数据集（含自建语料库、图像/视频/音频素材库、行业垂类数据集、高质量人工标注数据等），也包括数据标注方法（含标注规范、标注体系、标签层级设计、多人标注一致性校验机制等）、数据清洗办法（含去重去噪规则、低质数据过滤策略、有害与侵权内容识别规则、数据脱敏与合规处理流程等）、数据配比与采样策略（含多来源语料的混合比例、去重粒度与阈值设定等）；

（3）算法：

①核心算法逻辑与实现路径：如注意力机制变体、采样算法（DDIM、DPM-Solver 等）的改进方案、扩散过程调度策略、检索增强生成（RAG）的召回与重排算法；

②关键算法步骤与数据流向设计：算法各模块之间的调用顺序、数据传递路径、中间变量的取值与流转规则；

③算法选型与组合方案：针对特定任务在多种公开算法基础上的择优、嫁接与定制化改造思路；

④算法源代码及其中体现的非公知技术思路：包括函数实现细节、关键决策分支逻辑、容错与异常处理机制等。

（备注：算法的"思想层面"——如整体逻辑结构、决策路径、模块取值过程及调整思路——同样可以构成技术秘密点，并非只有源代码本身才受保护。）

（4）参数配置与方案：

①模型超参数：学习率及其调度策略、batch size、优化器选择与配置、正则

化系数、dropout 率、梯度裁剪阈值等训练超参数；

②推理参数：temperature、top-k、top-p、repetition penalty、采样步数（steps）、引导系数（CFG scale）、随机种子（seed）等生成控制参数；

③特定模块参数：LoRA/Adapter 的 rank 值与作用层选择、ControlNet 权重配置、VAE 参数、噪声调度（noise schedule）参数；

④参数调优方案：针对不同业务场景、不同输出风格、不同质量目标形成的参数组合方案与调参经验（俗称"炼丹配方"），以及参数之间的耦合关系与边界值设定。

（备注：单一参数本身可能不构成秘密点，但经长期试验调优形成的特定参数组合及其背后的取值依据通常具有非公知性和商业价值。其中随机种子本身通常不构成独立秘密点，其价值在于配合完整参数组合可复现特定输出，企业可以完整留存参数组合与种子记录，以备同一性比对时作为可复现性证据使用。）

（5）工作流：

①整体工作流编排：从用户输入到最终输出的完整 pipeline 设计，包括前置预处理、模型调用顺序、中间结果衔接、后置加工与质检的全链路节点编排（典型如 ComfyUI 节点图、Dify/Coze 等编排平台的工作流文件）；

②多模型/多模块协同方案：大模型与小模型协同（如"大模型+微算法"架构）、文生图+图生图+放大+修脸的多阶段串联、多 Agent 协作机制与调度策略；

③Prompt 工程方案：系统提示词（System Prompt）、提示词模板与变量体系、Few-shot 示例选取策略、提示词组合与权重配置、负向提示词（Negative Prompt）库等；

④检索增强与重排策略、知识库结构设计；质量控制与迭代机制：自动化评测

指标体系、人工审核节点设置、不合格内容的回流与再生成机制、A/B 测试与效果反馈闭环；

⑤工作流配置文件：以 JSON、YAML 等形式固化的工作流文件本身，及其中体现的节点连接关系与参数预设；

（6）智能体架构与技能资产：Agent 架构下的 Skill 及其工具定义与调用契约（工具描述、参数模式、返回结构与解析规则、错误与重试策略）；Agent 角色设定与系统指令、行为约束与安全规则及其版本迭代记录，不论以何种文件或存储形式固化；多智能体的职责划分、协同协议与调度策略；记忆与上下文管理方案（长程记忆结构、上下文压缩与淘汰策略、多轮状态维护机制）；

（7）评测与安全对齐体系：内部评测数据集及其构建方法、评分标准与评分细则、人工评测规范与评测员一致性校验机制、自动化评测流水线、模型能力基线与版本对比结论、红队测试用例库与对抗样本集，以及安全对齐规则与有害内容判定标准；

（8）其他：如算力调度方案、模型部署与服务化架构（含推理加速、负载均衡、缓存策略）、安全防护机制（含 prompt 注入防御、内容安全过滤规则）、与上下游系统的接口设计与集成方案，以及尚未公开的研发计划、技术路线图等。

### 2.3.2 产业链环节专属秘密点

（1）模型研发秘密点：模型结构、网络架构、表征形态、损失函数、收敛策略、注意力机制；训练方法、预训练/微调策略、蒸馏/量化/压缩方案、并行训练机制；训练数据采集、清洗规则、去重策略、标注规范、数据增强方案；软件架构、产品设计、3D 模型资产、制作工具、视觉表征方案；推理引擎、调度策略、加速方案、服务化封装、模型防窃取机制；端侧模型量化压缩、NPU/GPU

异构调度、端云协同推理、AI PC 硬件适配层设计、端侧模型防提取。

（2）工具服务秘密点：开源模型选型策略、测试评估报告、深度优化方法、微调参数、训练数据集设计；体系化提示词库、关键词模板、提示约束规则、精准提示组合策略、迭代升级机制；多源素材整合中间件、参数模板、工作流决策算法、模型兼容接口、上下文规范模板；异构数据解析引擎、素材去重/匹配/质检算法、跨平台同步机制、数据一致性保障策略；智能体角色划分、交互逻辑、多智能体（Multi-Agent）协同工作流、协同协议、资产一致性监督与修正方案；人员效率模型、工期预测算法、成本测算模型、资源调度与自动分配规则；项目系数配置、验收量化参数、合规风控阈值、内容审核与版权检索规则；历史项目库、人效数据库、客户特征库、错误案例库、行业基准数据库。

（3）内容制作秘密点：文本/语音驱动视频生成、跨模态映射、运动轨迹预测、音画智能对齐算法；视频智能拼接、剪辑点匹配、特效合成、主体与背景分离方法；超分修复、降噪增强、画质优化、风格迁移、虚拟形象生成方案；多轮交互意图迭代、场景一致性控制、成片校准、内容优化系统；未公开 IP、剧本、数字资产、特效模板、版权运营与内容风控策略。

# 第三章 AIGC 企业商业秘密常见泄密风险

指引结合 AIGC 行业发展特点，考虑技术研发、工具服务、内容制作全链条经营实际，综合参考人工智能行业秘密管理共性问题，系统梳理 AIGC 企业商业秘密主要泄密风险，包括行业共性泄密风险、AIGC 产业链不同环节企业特殊泄密风险、供应链及外部合作风险。

## 3.1 AIGC 行业共性泄密风险

本部分风险普遍适用于技术研发、工具服务、内容制作等全链条 AIGC 经营主体，是行业范围内高频、多发的基础性泄密隐患。

### 3.1.1 人员管理泄密风险

人员是商业秘密泄露的首要主体，也是各类泄密行为最核心的诱发因素。贯穿入职、在职、离职全周期。

（1）核心关键岗位泄密风险。算法研发、模型训练、技术架构、算力调度、核心商务、项目负责人等关键岗位人员，掌握企业核心算法、模型参数、技术路线、训练策略、定价体系、核心客户资源等涉密信息，易因离职跳槽、同业高薪诱导、内部矛盾、自主创业等因素，通过私自拷贝、云端留存、外接存储、线下传递等方式，故意带走或向外泄露商业秘密。

（2）普通员工安全意识不足泄密风险。企业常态化保密安全教育缺失，员工保密意识薄弱，日常办公中存在涉密文件随意转发、内部资料外发分享、私人设备处理工作涉密内容、公共场所讨论内部技术与经营事项等不规范行为，极易造成商业秘密无意识外泄。

（3）借助公共 AI 工具的无意识泄密风险。员工为图方便，把核心源代码、prompt、训练数据、客户资料粘贴进 ChatGPT、Claude、Codex、DeepSeek

等公共模型做调试或润色，数据可能进入对方训练池或被留存。

（4）权限管控失范泄密风险。中小微企业长期存在账号共用、访问权限无边界管控等问题；大中型企业存在岗位权限过大、超范围访问、调岗离职后权限未及时回收、超级管理员账号管控松散等漏洞，内部越权查阅、私自导出、批量下载涉密数据等问题。

（5）外部临时人员泄密风险。短期用工、实习人员、来访考察人员、临时技术支援人员准入审查不严、涉密范围未划定、未签订保密承诺，缺乏保密约束与全程监管，易近距离接触内部涉密资料引发泄露。

（6）AI 编程助手与开发工具插件泄密风险。研发人员使用 AI 编程助手、代码补全插件以及其他集成于开发环境的 AI 工具时，工具通常需要索引整个代码仓库，并在每次交互中将相关代码上下文发送至云端处理。企业未对此类工具实施统一管控的，核心源代码、密钥配置、提示词模板与模型配置可能在员工无感知的情况下持续外发，且该外发行为不体现为文件传输，常规数据防泄露措施难以识别。

### 3.1.2 数据全生命周期泄密风险

数据是 AIGC 产业的核心生产要素，训练语料、标注数据、模型参数、业务台账、客户信息等数据资产贯穿生产全流程，安全管控压力突出。

（1）数据存储安全风险。大量涉密数据集、模型权重、项目资料未采取加密存储、分级隔离、权限管控措施，服务器、本地终端、移动硬盘、U 盘等存储载体存在系统漏洞、防护缺失问题；多租户云存储环境数据隔离不彻底，离线备份介质保管松散，丢失、被盗、外流隐患较大。

（2）数据传输交互风险。AIGC 企业在内部跨部门协作、政企对接以及上

下游合作过程中，往往需要频繁传输模型文件、涉密报表、定制化方案等敏感信息。若未采用加密通道、身份核验、访问控制和传输完整性校验，相关数据可能在传输过程中被截取、监听、篡改或者非法留存。同时，业务 API 接口、数据交互端口和模型调用接口如缺乏访问限制、调用频次控制、异常行为监测等安全防护，可能遭受恶意爬取、非法注入、越权调用等攻击，造成批量敏感数据泄露。对于对外开放的模型服务，竞争对手还可能通过反复调用 API 实施模型逆推（Model Inversion）、成员推理（Membership Inference）、模型蒸馏、训练数据提取（诱导模型输出被记忆的训练内容）等攻击，反向获取训练数据特征或者复制模型能力，导致核心技术秘密外泄。

（3）数据使用管控风险。涉密数据未落实分类分级、脱敏处理、操作留痕管理，员工可随意查询、复制、导出核心数据；数据复用、外发、共享缺乏审批流程、使用限制、追溯机制，涉密数据无节制流转，进一步扩大泄密范围。

#### 3.1.3 开源软件使用泄密风险

AIGC 产业高度依托开源生态开展研发与迭代，开源框架、开源模型、第三方开源组件的广泛应用，形成行业特有泄密风险。

（1）自研技术与开源内容混同泄露风险。企业在开源模型基础上进行二次开发、参数调优、提示词工程改造、功能定制，未做好技术边界隔离，自研差异化优化方案、私有配置逻辑与开源代码混编，随代码对外流转造成自研核心技术被动泄漏扩散。

（2）开源代码提交失误泄露风险。研发人员操作不规范，误将包含私有算法、模型权重、业务涉密配置、项目核心逻辑的代码文件、脚本资料等上传至公共代码仓库、开源社区、公开网盘，造成涉密信息永久公开，损失难以挽回。

（3）开源依赖链安全隐患风险。开源项目依赖组件繁杂，部分第三方依赖库、插件存在隐藏漏洞、后门程序，可被外部攻击者利用突破系统防护，非法入侵后台、窃取业务数据与技术资料。

（4）开源协议与反向推演风险。部分开源协议具有传染性、强约束性，企业未合规研判协议条款,二次封装、商业化使用后被迫公开衍生代码与核心技术；竞争对手可通过解析企业对外开源内容、公开技术动态,反向推演企业研发方向、产品布局、核心技术短板。

### 3.1.4 信息发布与对外传播泄密风险

AIGC 行业技术交流频繁、行业分享活跃，对外宣传、学术交流、成果展示场景密集，主动披露环节易出现秘密管控漏洞。

（1）正式文稿过度披露风险。企业编制技术白皮书、行业研究报告、学术论文、专利申报材料、投融资计划书、招商资料时，未开展涉密审核与脱敏删减，过度披露模型架构、算法细节、训练逻辑、成本构成、盈利模式、独家合作资源等未受保护的商业秘密。

（2）非正式交流随意泄密风险。员工在行业峰会、技术论坛、直播分享、社交媒体、社群讨论、线下沙龙等场景，随意谈论内部研发进度、项目方案、定制化服务细节、客户合作内容，碎片化涉密信息叠加整合后，可被竞争对手完整还原核心业务逻辑。

（3）产品演示与公测泄露风险。企业在开放体验版模型、试用工具、公开演示系统或者公测环境时，如未设置必要的访问权限、调用限制、参数隐藏、内容脱敏和安全过滤机制，内置工作流模板、提示词规则、专属配置参数知识库内容等可能被外部用户抓取、测试、逆向拆解或者复刻模仿。外部主体还可能通过

提示词注入、越狱诱导、多轮试探等方式，诱导线上模型输出系统提示词（System Prompt）、内部工作流规则、知识库片段或者其他涉密配置信息，进而削弱企业差异化竞争优势并造成商业秘密外泄。

### 3.2 AIGC 企业特殊泄密风险

结合 AIGC 企业上游、中游、下游差异化业务模式、核心资产与运营场景，各环节存在特殊泄密风险。

#### 3.2.1 上游模型研发企业特殊泄密风险

上游以大模型研发、算法创新、算力调度、基础模型训练为核心业务，泄密风险集中于核心技术与研发资料。

（1）核心研发成果泄露风险。模型网络架构、预训练逻辑、损失函数设计、训练迭代策略、蒸馏压缩方案等底层核心技术，是企业核心竞争壁垒，易被核心研发人员私自留存或被同业竞争者非法获取。模型权重、参数文件、专属训练数据集、差异化微调方案等一旦泄露，将直接削弱企业技术领先优势。企业对外提供模型 API、评测接口或试用服务时，如缺乏调用频次控制、异常查询监测和输出限制，竞争对手还可能通过反复调用接口、构造查询样本、拟合输出结果等方式实施模型蒸馏，变相复制模型能力或还原关键行为特征，造成核心研发成果外泄。

（2）研发过程资料泄露风险。实验日志、对比测试数据、消融实验结论、训练失败记录、调参经验、技术迭代草稿、未公开研发方案等过程性资料，虽然未必直接体现为最终产品形态，但往往能够反映企业技术路线、研发取舍和核心经验。如果未纳入保密管理，随意存放、流转或共享，可能被外部主体整合分析后还原企业研发思路，形成泄密隐患。

（3）算力与训练环境泄露风险。上游企业通常依托专属算力集群、私有化部署环境、训练平台和代码仓库开展模型训练。若网络隔离、访问权限、账号密钥和操作日志管理不到位，外部人员可能非法接入训练环境，抓取训练日志、运行参数、模型中间版本以及训练中间检查点（checkpoint）等关键载体。上述信息一旦被获取，可能暴露模型训练进度、参数状态、优化方向和阶段性技术成果，甚至被用于恢复、复现或继续训练相关模型。

### 3.2.2 中游工具服务企业特殊泄密风险

中游聚焦 AIGC 工具开发、模型适配、接口服务、流程定制等，泄密风险集中于适配技术、调度逻辑与运营规则。

（1）定制化适配技术泄露风险。针对不同开源模型、业务场景开发的中间件程序、跨平台适配接口、工作流调度算法、批量处理规则，是工具企业核心资产，易被反向工程拆解、合作方越权获取。

（2）提示词工程与模板泄露风险。体系化提示词库、场景化 prompt 模板、内容生成调控规则、风险过滤逻辑，属于高价值经营秘密，一旦外泄易被同行直接复制套用。

（3）平台运营权限泄露风险。API 密钥、接口调用规则、计费配置、权限分配体系、租户管理策略管控不当，易出现非法调用、盗用服务、篡改配置等行为，引发业务数据与运营规则泄露。

### 3.2.3 下游内容制作应用企业特殊泄密风险

下游依托 AIGC 工具开展图文、音视频、虚拟内容、营销文案等定制化生产，泄密风险集中于内容资产、客户项目与运营经营信息。

（1）专属内容资产泄露风险。原创创作模板、风格化参数、素材资源库、

虚拟形象设计方案、未公开 IP 内容、定制化剪辑合成流程，多为非标化独有资源，在外包协作、素材共享中容易被私自留存传播。

（2）项目涉密信息泄露风险。定制化客户需求、项目实施方案、服务报价体系、优惠政策、履约细节、合作底线等经营信息，直接关联市场竞争，管控缺失易被竞品获取。

（3）内容生产流程泄露风险。专属生产流水线、质量管控标准、内容审核规则、批量生产优化方案等内部管理秘密，随着人员流动、外包对接发生泄露。

### 3.3 供应链及外部合作泄密风险

AIGC 产业算力需求大、外包场景多、上下游协作紧密，硬件、数据、云服务、软件工具、外包服务共同构成外部泄密主要渠道。

#### 3.3.1 软硬件供应链泄密风险

（1）硬件设备安全风险。模型训练、渲染运算依赖的高性能服务器、AI 加速芯片、边缘计算设备、存储硬件等硬件设备，存在隐性后门、未披露漏洞的风险，在长期运行过程中隐秘采集运算日志、运行参数、架构信息，易造成技术秘密隐性泄露。

（2）软件工具链风险。研发设计、内容生产、运维管理所使用的第三方工具、插件、数据库软件、调度系统来源繁杂，如果未开展安全检测与准入审核，恶意代码、隐藏漏洞可能被利用，导致非法读取本地涉密文件、后台业务数据等后果，引发泄密风险。

#### 3.3.2 数据与外包服务泄密风险

AIGC 企业可能将数据清洗、文本标注、图像标注、内容审核、素材加工等基础业务外包，外部作业团队长期接触原始训练数据、行业专属语料、涉密素材

资料。若外包合作未签订专项保密协议、未明确涉密边界、未落实数据脱敏、操作留痕、权限隔离等管控措施，外包人员可私自复制、留存、外传敏感数据，形成常态化泄密漏洞。部分外包方还可能超出合作目的，将企业提供的涉密数据、标注成果或业务素材用于训练、微调自有模型，导致企业数据资产被不当吸收、沉淀并转化为第三方模型能力，进一步扩大商业秘密外泄后果。

#### 3.3.3 云服务与第三方平台泄密风险

多数 AIGC 企业依托公有云、第三方算力平台完成模型训练、推理部署与数据存储。云服务多租户架构下，权限配置错误、存储桶公开、容器镜像夹带涉密资料、访问策略宽松等问题，易导致私有化模型、业务数据、配置文件被公开暴露。在云端训练或微调过程中，训练数据、模型权重、参数文件、检查点及运行日志需要经第三方平台存储、调度或流转，如缺乏专用环境隔离、加密传输、访问审批和日志审计，相关核心资产可能被越权访问、违规导出或长期留存。第三方算力平台、托管运维机构人员权限过大、内部管控不严的，也可能引发企业涉密资产外泄风险。

#### 3.3.4 上下游合作方泄密风险

企业在技术共建、模型对接、业务联营、渠道合作过程中，需向合作方开放接口权限、共享技术方案、同步业务规则。但目前存在合作边界模糊、保密条款约定笼统、涉密资料交付无管控等问题，易导致合作方可超合作范围擅自使用、复制、扩散涉密信息；且合作终止后，未及时回收权限、清理涉密资料，造成商业秘密长期存在持续泄露隐患。

#### 3.3.5 第三方中转接入服务泄密风险

部分企业通过第三方中转、代理接入等方式使用境外模型服务。此类模式下，

企业的提示词、上传文件、业务数据与模型输出需经中转服务方解析与转发，中转服务方在技术上具备获取上述内容明文的条件，其是否留存、复用相关内容，企业不具备技术核验手段。同时，中转服务方持有与上游服务商之间的真实凭证，上游服务商作出的数据保护与不留存承诺，其相对方为中转服务方而非企业，不直接及于企业。此外，此类模式下数据出境合规义务亦难以落实。上述因素叠加，可能导致核心商业秘密在企业不知情的情况下被留存、复用或者外泄。

# 第四章　AIGC 企业商业秘密内部管理体系

AIGC 企业商业秘密内部管理体系是企业落实保密责任、防控泄密风险、保障创新成果安全的核心制度支撑。企业应立足业务实际，建立流程规范、动态适配、运行高效、权责清晰的内部管理体系，将商业秘密保护全面融入研发、运营、合作、管理各环节，实现全主体、全流程、全要素闭环管理。

## 4.1 AIGC 企业商业秘密内部管理体系的定位

AIGC 企业商业秘密内部管理体系，是企业为保护核心商业秘密，构建的集组织、制度、技术于一体的综合管理系统。管理体系应当与企业经营规模、业务类型、研发特点、风险状况相适应，坚持保护与发展并重、安全与效率协同，推动商业秘密保护与技术创新、产业应用深度融合，为企业持续健康发展提供坚实保障。

### 4.1.1 管理策略

企业可以结合 AIGC 行业技术迭代快、数据要素集中、开源应用广泛、协作链条长等特点，制定科学完善的商业秘密管理策略。

（1）精准匹配保护。根据商业秘密的价值、重要程度及泄密风险等级，实施差异化保护，确保保护措施与秘密重要性相适配，兼顾安全保障与运营效率。

（2）最小知悉管控。严格按照岗位必要原则限定涉密信息知悉范围，规范访问权限，严控核心秘密流转，从源头降低泄密风险。

（3）全生命周期管理。覆盖商业秘密产生、存储、使用、传输、复制、归档、解密直至销毁全过程，明确各环节责任人员及管理要求，实现全程可管、可控、可追溯。

（4）动态优化调整。结合技术升级、业务拓展、场景更新及外部风险变化，定期评估管理体系运行效果，及时优化策略、制度与措施，保持保护效能持续适配。

#### 4.1.2 管理模式

企业可根据自身规模、业务布局、组织架构和风险特点，选择适合的商业秘密管理模式，可单独适用或组合实施。

（1）部门管理。按照研发、技术、运营、市场、数据、内容等职能分工，明确各部门保密责任，实行谁产生、谁负责、谁管理。

（2）人员管理。根据岗位涉密等级实施分类管理，对核心涉密人员、重要涉密人员、一般涉密人员设置差异化管控要求，强化全流程约束。

（3）项目管理。针对模型研发、定制化开发、场景部署、内容制作等项目实施专项保密管理，明确项目保密责任与信息管控要求。

（4）阶段管理。结合研发、训练、微调、部署、运营、合作等不同业务阶段，设置阶段性保密重点，实施阶段化精准防控。

（5）跨部门协同管理。建立跨部门联合审查、会商研判、风险共控机制，对技术发布、开源提交、对外合作、数据共享等重大事项实行多部门联审，守住安全底线。

#### 4.1.3 组织架构

企业可结合自身规模与业务特点，建立层级清晰、分工明确、协同联动的商业秘密保护组织架构，保障管理体系有效运行。

**最高管理层：**企业最高管理层对商业秘密保护承担最终责任，负责确定商业秘密保护战略与方针，审定重要制度与重大事项，保障人员、经费、技术等资源

投入，推动形成重视保密、遵守制度的企业文化，统筹处置重大泄密事件。

**管理部门：**企业可结合自身部门设置与业务特点，明确商业秘密保护归口管理部门，可设立知识产权、法务、技术安全或综合管理相关机构。主要职责包括：组织制定保密制度与规范，开展定密管理、保密培训、监督检查、风险排查、泄密事件处置及跨部门协调，推动各项保护措施落地实施。企业可根据规模配备专职或兼职管理人员。

**责任部门：**研发、技术、数据等各业务部门，是商业秘密保护的直接责任部门。各部门应严格执行保密制度，规范本部门涉密信息管理，落实岗位保密要求，配合开展检查、培训与整改工作，及时报告风险隐患。

**跨部门协同：**企业可结合自身部门设置与业务特点，建立健全跨部门协同机制，完善信息共享、会商研判、联合审核流程。针对核心技术对外交流、模型展示、开源发布、第三方合作、数据对外提供等高风险事项，实施多部门会签审核，强化协同防控，补齐管理短板，形成全流程、一体化保护格局。

### 4.2 AIGC 企业商业秘密内部管理体系的制度安排

AIGC 企业商业秘密内部管理体系的制度安排，围绕商业秘密的确定与分类分级、涉密人员、涉密载体、涉密区域、泄密预警与应急处置、争议处置与奖惩、第三方合作、技术安全措施等方面展开，覆盖商业秘密管理的关键环节。企业可结合自身经营规模与业务特点，将各项制度落实到岗位、流程与技术手段中，形成可执行、可追溯、可验证的管理闭环。相关制度的建立与执行情况，是认定企业是否已采取相应保密措施的重要依据。

#### 4.2.1 商业秘密的确定与分类分级

企业可结合自身部门设置与业务特点，建立商业秘密确定与分类分级管理机

制，通过规范定密、分类分级、解密管理与动态调整，实现商业秘密精准识别、有效管控、定期评审和持续优化，提升保护工作的系统性与适用性。

#### 4.2.1.1 定密制度

企业可结合自身部门设置与业务特点，建立常态化定密工作机制，明确责任主体、工作标准与实施流程，全面梳理具体技术信息和经营信息，将符合条件的信息纳入商业秘密管理范围。

（1）明确定密责任主体。企业应指定定密负责人或定密工作小组，组织各业务部门开展信息梳理与密点识别，按照信息的性质、用途和重要程度完成初步密级判定，并统一登记归档。定密负责人可由高级管理人员、核心业务部门负责人或商业秘密管理部门负责人担任。

（2）明确密点。企业可结合企业模型、算法、参数配置方案、客户名单等信息业务范围，根据自身经营实际与发展需要开展全面梳理与精准识别。

（3）明确密级。企业可根据信息价值、泄露危害程度、竞争影响和反向工程难度等因素，将商业秘密划分为核心秘密、重要秘密、一般秘密三个等级，并结合自身业务规模设定合理的泄密损失判定标准。

（4）设定保密期限。企业可根据技术迭代周期、市场窗口期和信息有效生命周期确定保密期限，能够明确具体期限的按照实际期限标注，无法确定具体期限的可确定为长期保密，并定期开展价值评估。

（5）管理审批与登记。定密结果应当履行内部审批程序，经批准后实施统一登记、统一标识和统一管理。企业可建立商业秘密登记簿，完整记录秘密事项、密级、保密期限、知悉范围、存储位置、版本信息和保管责任人等内容，确保全程可追溯、可核查。

（6）管理密点标识。对纸质文件、电子文档、代码库、数据集、模型文件等各类载体作出清晰密级标识，保证涉密信息可识别、可区分和可管控。

#### 4.2.1.2 分类分级管控制度

企业应按照分类清晰、分级精准、措施匹配的原则，对商业秘密实行差异化管控，确保保护力度与风险等级相适应。

（1）实施分类管理。企业可以根据商业秘密的属性与运行场景，实施对应的管理规则。技术信息重点围绕研发生成、存储使用、传输交互、代码管理以及模型部署等环节，强化技术层面的防护。经营信息重点围绕知悉范围控制、内部流转审批、对外披露审核以及合作信息管理等环节，强化流程层面的约束。不同类别的商业秘密实行分开台账、分开管控和分开审批，确保管理边界清晰、责任明确。

（2）实施分级管控。企业可以根据商业秘密的重要程度与泄露影响，实施梯度化管控。核心秘密实行最严格的知悉范围限制、访问权限控制以及操作留痕管理。重要秘密强化访问审批、传输加密以及使用监督。一般秘密落实规范标识、日常管理以及风险监测。不同密级对应实行差异化的场所管理、权限管理、载体管理以及对外交流管理。

（3）落实最小授权管理。企业可以按照岗位必需与职责匹配原则，合理设置信息访问权限。权限配置与密级相对应，与岗位相适应，与工作相协同。企业严格管控超范围授权、超权限访问以及超用途使用行为，确保涉密信息始终处于可控可管状态。

#### 4.2.1.3 解密制度

企业可结合自身部门设置与业务特点，建立规范的解密审查与退出机制，及

时对失去保护价值或者已经公开的信息解除保密管理，避免过度保护影响技术迭代与业务运行效率。

（1）开展定期审查。商业秘密管理部门可定期组织全量商业秘密的价值复核，重点关注技术公开状态、替代技术进展、市场价值变化以及业务调整方向。针对 AIGC 领域技术迭代快、开源更新频繁的特点，企业可提高审查频次，及时判断相关信息是否仍具备保密必要。

（2）明确解密适用情形。已经为公众所知悉、相关技术被替代或者公开、相关经营信息不再具有保护价值、相关业务已经终止且无后续利用必要的、企业根据经营发展需要决定不再保护的信息可以予以解密。

（3）规范解密申请与审批。解密由业务部门或者原定密责任人提出申请，说明具体依据和理由，经商业秘密管理部门审核并按照内部权限完成审批后正式生效。涉及模型算法、训练数据、核心代码等关键技术解密的，应当加强多部门联合研判。

（4）做好标识与档案更新。企业应当及时清除解密信息的密级标识，更新商业秘密登记簿，并同步告知相关岗位人员。解密信息仍具备参考或者存档价值的，按照企业档案管理规定继续妥善保存与合理使用。

#### 4.2.1.4 动态调整

企业可结合自身部门设置与业务特点，建立商业秘密全周期动态管理机制，实现定密、管控、解密的闭环运行，确保管理体系持续适配 AIGC 行业发展与企业经营实际。

（1）定期组织复评调整。商业秘密管理部门应当定期开展全面复评，结合技术迭代、业务拓展、市场竞争变化、合作模式调整以及开源生态演进，及时调

整商业秘密的范围、密级、保密期限和管控措施。复评周期可与商业秘密的密级相适应，核心秘密的复评频次高于重要秘密和一般秘密。发生基础模型更换、技术路线重大调整、核心产品形态变更、重要合作关系建立或者终止、所依赖开源项目发布重大版本或者其许可协议变更、企业自研技术方案被第三方以预印本论文或者开源代码等方式先行公开，以及行业出现颠覆性技术范式变化等情形的，应当及时启动专项复核。企业宜建立对所依赖开源项目与相关技术领域公开动态的常态化跟踪机制，为专项复核提供触发信息来源。

（2）实施动态升降级管理。涉密程度提升的信息应当及时升级密级并强化保护措施。保护价值下降或者已经公开的信息应当及时降级或者解密。企业重点关注模型版本更新、数据迭代、场景拓展、技术公开等情形，快速响应变化并优化管理要求，不断提升商业秘密保护的精准性和有效性。

#### 4.2.2 涉密人员管理制度

企业可结合自身部门设置与业务特点，建立覆盖入职、在职、离职全流程的涉密人员管理机制，对涉密岗位密集、涉密信息价值高、人员流动频繁的岗位实施全周期、可追溯、可管控的人员保密管理，从源头降低泄密风险。

##### 4.2.2.1 招聘与入职

企业可结合自身部门设置与业务特点，加强涉密人员招聘与入职管理，严把人员准入关，确保涉密人员具备相应保密意识。

（1）规范招聘筛选。企业在招聘涉密岗位人员时，可开展必要的背景审查，重点了解应聘人员工作经历、履职情况以及与原单位的保密约定等内容。企业可评估应聘人员的保密意识与职业信用，避免聘用存在泄密风险或不适宜接触核心信息的人员。对于核心技术、核心研发、数据管理、算法设计等关键岗位，应当

强化审查力度，确保人员背景清晰、风险可控。

（2）完善入职协议签订。新员工入职时，企业可以制度告知、协议签署等方式，明确保密范围与保密义务，并确保相关内容有效送达员工并留存记录。企业应当根据岗位涉密程度，与涉密人员签订保密协议。对高级管理人员、核心技术人员以及其他掌握重要商业秘密的人员，可以同步签订竞业限制协议，明确双方权利义务，强化核心信息保护。

#### 4.2.2.2 在职管理

企业可结合自身部门设置与业务特点，加强涉密人员全流程日常管理，推动保密要求融入岗位职责与业务运行。

（1）强化日常管理。企业应当督促涉密人员严格遵守保密制度，规范涉密信息使用、存储与流转行为。员工应当按照要求使用与保管涉密信息，离开岗位时及时关闭相关系统或做好安全防护。企业可为涉密人员设置独立账号并开启行为日志记录，根据岗位需要开放最小必要权限，确保操作可追溯、可核查。

（2）加强培训与考核。企业可将商业秘密保护培训纳入常态化管理，面向涉密人员开展针对性培训，内容包括保密义务、保密范围、风险防范以及法律责任等。企业可以采取集中培训、线上学习等多种方式开展培训，并完整保存培训材料与相关记录。培训后可组织必要考核，提升涉密人员保密意识与实操能力。

（3）规范员工转岗管理。员工发生岗位调整时，企业可根据新的岗位职责重新核定涉密范围与访问权限，及时调整系统权限并更新涉密人员管理台账。确有需要的，应当重新完善保密相关约定，确保保密管理与岗位变动同步衔接。

#### 4.2.2.3 离职管理

企业应当对涉密人员离职实施严格管控，防止涉密信息随人员流动发生泄

露。

（1）规范工作交接。涉密人员离职前，应当完整移交所有涉密资料、数据、载体、设备及相关账号信息。企业应当逐项核对交接内容，确保涉密资产全部回收、无遗漏、无私自留存。对核心研发、数据管理、算法设计等关键岗位员工，可设置合理交接周期，平稳降低信息接触权限。

（2）强化权限回收与技术清理。员工离职后，企业应当立即关闭并注销所有系统账号，逐项轮换其可能持有的各类凭证，包括模型服务 API 密钥、云平台访问密钥、代码仓库与制品库的个人访问令牌、SSH 公钥、容器镜像仓库凭证、数据库与向量库账号、Webhook 密钥，以及已下发至持续集成流水线的凭证，阻断一切访问路径。企业应当对离职人员使用过的设备进行全面清理，清除涉密数据并排查异常传输、下载、拷贝等行为，防范信息被私自带走或外传。

（3）落实竞业限制与持续关注。对签订竞业限制协议的人员，企业应当在离职时再次明确相关义务，并按约定履行支付补偿等责任。企业可以在合法合规前提下，关注离职人员从业去向与业务动态，及时发现潜在泄密或侵权风险，维护自身合法权益。

#### 4.2.3 涉密载体管理制度

企业应当建立全流程涉密载体管理机制，对记载商业秘密的各类介质实行统一分类、标识和管控，确保载体从制作、使用、保存到销毁全程可控可追溯。

（1）规范涉密载体分类。涉密载体包括以电子形式存储涉密信息的各类设备，也包括以文字或图形等形式记录涉密信息的纸质资料。电子载体涵盖计算机、服务器、训练设备、存储设备、移动介质、云存储空间以及各类智能终端。纸质载体涵盖内部文件、设计图纸、实验记录、研发文档等。企业应当根据载体形态

与使用场景实施分类管理。

（2）明确载体管理要求。企业应当根据涉密等级对载体进行清晰标识，明确管理责任与使用权限。载体使用应当履行内部审批程序，长期使用的载体开展定期检查，临时使用的载体严格审核使用必要性。企业可完整记录载体使用过程，形成使用日志并妥善归档。员工应当熟悉载体保密要求，按照规定规范操作与保管。员工岗位调整或离开企业时，应当及时交还全部涉密载体并接受全面检查。

（3）强化数据备份与恢复。企业应当建立稳定可靠的数据备份与恢复机制，保障涉密数据安全完整。企业可以对数据访问行为进行全程日志记录，及时发现异常访问与异常操作。定期开展安全审计与风险排查，修复系统漏洞，防范外部攻击与数据丢失风险，保障涉密信息持续可用。

（4）规范废弃载体处置。退出使用的涉密设备与存储介质不得随意丢弃或自行处置。企业应当按照保密要求进行物理销毁或通过专业机构实施安全处理，确保信息不可恢复。涉密设备改作其他用途前，必须完成全面数据清除与安全检测，杜绝信息残留泄露。对固态存储介质，多次覆写的方式不足以保证数据不可恢复，企业应当采用厂商提供的安全擦除指令、对全盘加密介质销毁密钥的方式，或者直接实施物理销毁。对 GPU 训练节点，企业在退役或者退租前还应当清理显存缓存、本地临时目录、检查点缓存与容器镜像层残留。

#### 4.2.4 涉密区域管理制度

企业可以根据商业秘密保护需要，合理划定涉密区域并实施严格物理管控，构建安全可靠的涉密活动空间，防范信息窃取行为的发生。

（1）科学界定涉密区域。涉密区域是指集中处理、存储、研发商业秘密的物理场所，主要包括模型训练机房、数据中心、实验室、研发办公区、档案室、

服务器间等。企业可以结合业务布局与涉密信息分布，明确区域范围与管控等级，形成层次清晰的区域管理格局。

（2）落实区域管控措施。企业可以对涉密区域采取有效物理隔离，设置符合安全要求的门禁系统，核心涉密区域实行双人验证或多级授权管理。涉密区域入口应当设置明显警示标识，明确禁止行为与管理要求。企业可以对涉密区域实施全程监控与安全巡查，保证监控设备正常运行并规范留存记录。

（3）规范人员进出管理。企业员工应当熟悉涉密区域管理要求，严格按照授权范围开展活动。非相关人员进入涉密区域应当履行审批程序，企业对进入人员进行告知提醒并限定活动范围。外部人员进入核心涉密区域，应当在专人陪同下开展活动并做好登记，确保区域内信息安全可控。

（4）落实逻辑涉密区域管控。企业可以对模型训练与推理环境、代码仓库、模型仓库、数据湖与向量数据库、持续集成与交付流水线等逻辑涉密区域，实施与物理涉密区域同等强度的管控。相关接入应当通过统一入口进行，企业可以禁止绕过统一入口的直连，并对接入会话实施操作录制与留痕。

#### 4.2.5 泄密预警和应急处置制度

企业可结合自身部门设置与业务特点，建立全流程泄密预警与应急处置制度，在出现泄密情形时最大限度降低泄密造成的影响与损失。

（1）健全泄密预警制度。企业可以构建常态化风险监测体系，对涉密信息访问、传输、存储等行为进行持续跟踪。通过系统日志审计、异常操作识别、权限变动监控、数据外发拦截等技术手段，及时发现账号异常登录、非工作时间批量下载、违规拷贝、异常传输等风险信号。企业可以明确预警触发标准、报送路径与处置时限，确保风险隐患在萌芽阶段得到有效处置。针对模型训练环境、核

心代码库、训练数据集、API 接口等高风险场景，应当强化实时监测与自动预警能力，提升预警精准度与响应效率。

（2）完善应急处置制度。企业可结合自身部门设置与业务特点，制定泄密事件应急预案，明确组织指挥、部门职责、处置流程与操作规范。发生泄密或存在重大泄密风险时，应当立即启动应急机制，由商业秘密管理部门牵头，技术、法务、人力、网络安全等部门协同开展工作。技术部门负责通过日志追溯、数据水印、行为分析等方式定位泄露源头与扩散范围；网络安全部门及时采取权限冻结、连接阻断、设备封存、数据撤回等措施，控制风险扩大；法务部门开展法律风险评估，固定相关证据，必要时向监管部门报告或启动维权程序；人力资源部门对涉事人员采取权限管控、设备核查等措施，依规开展内部处理。此外，企业应当留存完整应急处置记录，事件处置后及时开展复盘分析，查找管理漏洞与薄弱环节，优化制度流程与技术防护措施，避免同类问题重复发生。

#### 4.2.6 争议处置和奖惩制度

企业可结合自身部门设置与业务特点，建立规范有序的商业秘密争议处置制度与公平明确的奖惩制度，保障商业秘密内部管理体系的有效落地执行，维护企业合法权益与正常管理秩序。

（1）规范争议处置制度。企业可以完善商业秘密相关争议的内部处理流程，明确受理、调查、审议、结论、执行等环节要求。发生泄密争议或侵权纠纷时，企业可综合运用代码比对、数据溯源、操作日志分析等技术手段开展事实认定。企业应当注重证据固定与留存，完善协议管理、存证记录、行为审计等基础工作，为内部处理与外部维权提供支撑。争议处理过程中应当坚持客观公正，兼顾合规要求与合理诉求，妥善化解内部管理纠纷。涉及外部侵权的，企业可综合运用行

政投诉、民事追偿、刑事报案等途径维护权益，必要时借助专业法律服务与技术鉴定机构支持，提升争议处理效果。

（2）健全奖惩制度。企业可结合自身部门设置与业务特点，建立与保密工作挂钩的奖励机制，对在保密工作中表现突出的部门和个人给予表彰奖励，并通过合同或企业管理规章制度进行落实。一方面，对积极参与保密管理的人员进行奖励。重点奖励主动发现并报告系统漏洞、有效规避重大泄密风险、提出合理改进建议、提供侵权重要线索、积极参与泄密处置的人员，激励全员参与保密管理。另一方面，明确分级惩戒标准。对违反保密制度、违规操作、不当使用、擅自披露、窃取泄露商业秘密等行为，根据情节轻重与危害后果给予相应处理。存在一般违规情形的，给予提醒教育、警告通报、绩效处理等处分；造成较大风险或一定损失的，给予调岗、降职、解除劳动关系等处理，但相关处理应符合劳动法规定及劳动合同相关约定。故意泄露核心商业秘密、造成重大损失或严重影响，涉嫌违法犯罪的，依法移送司法机关追究责任。奖惩结果应当纳入员工管理档案，与考核、任用、晋升等挂钩，推动保密责任落到实处。

#### 4.2.7 第三方合作管理

企业可结合自身部门设置与业务特点，建立全流程第三方合作保密管理制度，强化合作前、合作中、合作后全周期风险防控，防范与第三方合作过程中的商业秘密泄露。

（1）明确合作界定与全域管理范围。第三方合作涵盖与企业无隶属关系的各类主体往来，包括商务协作、联合研发、服务外包、技术咨询、中介服务、国际合作等业务形态。企业应对所有可能接触商业秘密的外部合作与外部人员访问实施统一管理。

（2）严格外部人员访问管理。外部人员进入企业应当出示有效证件并完成登记，佩戴与内部员工相区分的专属出入凭证。外部人员进入涉密区域须经过内部审批并再次登记，企业应当明确告知禁止录音、摄影、摄像及携带移动存储设备等要求，对相关设备进行必要限制并安排专人全程陪同。企业可划分可参观区域与禁止参观区域，设置专用参观路线，避开核心涉密场所，对路线沿途可能暴露的涉密信息采取隐蔽处理。

（3）规范项目合作全流程管理。企业开展涉及商业秘密的活动时，应当与合作方签订保密协议，或在合作合同中设置专门保密条款，明确保密范围、保密义务、使用限制与违约责任。共同研发或委托研发项目开展前，应当对合作方进行背景与保密能力评估，同时防范自身行为侵犯第三方合法权益，并在协议中明确知识产权归属与使用边界。涉密项目需长期向外部提供信息或频繁进入涉密区域的，企业可要求参与项目的外部人员签订个人保密承诺，使用企业统一提供的涉密计算机、加密系统与加密存储介质，并对外部携带设备进行安全检查。

（4）强化涉密会议及活动管理。举办涉及商业秘密的内部会议或外部活动，应当选择具备安全保障条件的场所。尽量采用线下方式开展，确需使用线上方式的，应当设置会议密码、屏幕水印等安全防护措施。企业可根据工作必要性限定参会范围，告知参会人员保密要求，必要时签订保密承诺书。加强会议涉密文件管控，明确发放范围并做好登记，重要文件标注回收标识，会议结束后及时清点回收。

（5）落实准入、协议与履约全链条管控。企业建立第三方合作准入与动态考核机制，加强合同履行与保密执行情况跟踪。合作前开展知识产权与合规尽职调查，合作中严格信息提供审批与权限控制，合作终止后及时回收信息、销毁或

返还涉密载体，确保合作全程风险可控。

#### 4.2.8 技术安全措施

企业可以结合 AIGC 业务技术特点，构建覆盖网络、系统、软件、数据全链条的技术安全防护体系，以技术手段强化商业秘密安全保障能力。

（1）强化网络安全防护。企业应当部署符合安全要求的网络防护设施，建立边界防护、访问控制、终端准入等多层次防护机制。对模型训练环境、核心服务器、数据中心、代码管理平台等关键部位实施重点防护，严格控制外部接入，实现网络访问可管可控、操作行为可追溯可审计。模型训练与推理环境除控制外部接入外，还应当对出站方向实施白名单管控，限制训练节点直接访问公网，并对对象存储空间的批量读取行为单独监测。对模型权重、训练检查点、数据集等大体积文件的读取与出站传输，企业应当建立基线并配置异常告警。

（2）保障业务系统安全运行。企业应当规范使用各类业务管理系统、研发系统、办公系统与数据共享平台，强化系统权限管理、操作留痕与安全加固。针对代码管理、模型管理、数据管理、文档管理等核心系统，实行分级授权与安全管控，确保系统运行稳定、数据流转安全。

（3）加强软件安全管理。企业可以对办公、研发、生产使用的各类软件开展安全评估，及时更新版本并修复安全漏洞。严格执行软件授权管理，禁止未经许可安装、复制与使用非合规软件，防范恶意程序、后门漏洞带来的泄密风险。研发类软件与工具应当纳入统一管理，确保来源可靠、配置安全。企业可以对基于开源模型、开源框架的二次开发成果建立独立的代码库与版本管理，将自研微调参数、适配层、提示词工程方案与开源底座隔离存放并单独定密，形成清晰的自研技术边界。企业宜将开源底座以外部依赖方式引入，不将底座源码复制进自

研仓库；建立软件物料清单并将开源许可扫描纳入代码审计，对具有传染性的开源许可在合入前予以阻断并触发人工评审；对外交付或者开源时，仅发布对底座的引用而非微调增量本体。企业还可以对 AI 编程助手、代码补全插件等集成于开发环境的 AI 工具实施统一管控，统一采购具备企业级数据保护条款的版本并通过企业租户管理成员，关闭代码用于模型训练与产品改进的选项，配置仓库级排除规则以隔离核心模块、密钥与数据文件，并谨慎授权员工以个人账号在涉密仓库中使用此类工具。

（4）落实 AIGC 专项技术处理。企业可以在数据处理、模型训练、内容生成等关键环节采取针对性技术保护。对训练数据与业务数据开展脱敏处理与权限管控，采取有效措施防范模型逆向解析、窃取、破解等风险。企业还可以同步部署模型与数据溯源技术措施，包括模型权重水印、训练数据指纹、生成内容隐式标识、API 调用行为指纹等。相关措施既可提升泄密发现能力，也可在后续维权中作为权属归属与同一性比对的证据支撑。

### 4.3 AIGC 企业商业秘密维权准备

企业可结合自身部门设置与业务特点，建立完善的商业秘密维权应对机制，做好事前评估、证据固定、路径选择与抗辩准备，提升维权规范性与有效性。建立维权应对机制时，建议企业从自身作为权利人和被控侵权方两个维度进行准备。

#### 4.3.1 权利人维权准备

企业作为商业秘密权利人，发现商业秘密疑似遭受侵害时，应当有序开展维权准备工作，为后续救济奠定基础。

（1）开展侵权评估。企业应当及时对疑似侵权情形开展综合判断，明确被

侵害信息属于技术信息或经营信息，梳理侵权行为的具体表现形式，确定侵权嫌疑主体身份及其与企业的关联关系，判断信息扩散范围与传播途径。结合研发投入、市场影响、技术贬值、客户流失与商誉受损等情况，评估侵权造成的实际危害与潜在风险，形成完整评估结论。

（2）规范证据收集。企业可以系统固定与维权相关的各类材料，确保证据真实合法且相互关联。

第一，准备主体资格材料（营业执照、许可合同、授权委托书等）。证明自身享有相关商业秘密权利及提起维权的合法权限。

第二，明确被投诉方身份信息（自然人姓名、性别、年龄、住址等个人信息、法人或其他组织工商登记信息）及身份证明材料（身份证、营业执照等）。确保指向清晰。

第三，准备权利基础证据。证明相关信息符合商业秘密法定构成要件，包括信息具体内容、形成过程、秘密状态、商业价值以及企业已采取的保密措施。

第四，收集侵犯商业秘密的初步证据。证明涉嫌侵权人有渠道或有机会获取商业秘密，其使用的信息与企业商业秘密构成实质相同，以及相关信息已经被非法获取、披露或使用。

第五，收集受到损害后果的证据，包括经济损失、侵权获利、合理许可费用以及维权合理开支等相关凭证。证据收集过程可在专业机构或监管部门指导下开展，必要时通过公证等方式进行固定保全。

企业可根据侵权情节、危害程度与自身需求，选择民事追偿、行政投诉、刑事报案等适当途径维护合法权益，确保维权行为依法有序、高效有力。

#### 4.3.2 被控侵权方维权准备

企业被主张侵犯商业秘密时，应当依法开展抗辩准备，在查明事实基础上提出合理抗辩理由，维护自身合法权益。

（1）商业秘密不成立抗辩。企业可围绕商业秘密法定构成要件，提出相应抗辩理由。包括：秘密性，相关信息已为公众所知悉，属于行业常识或公开信息，不具备秘密性；无保密措施，权利人未采取与其商业价值相匹配的合理保密措施，相关信息不满足保密性要求；不具有价值性，相关信息不具有现实或潜在商业价值，无法为权利人带来竞争优势。

（2）合法来源抗辩。企业可通过证明信息来源合法，主张不构成侵权。包括：自行研发，相关信息由企业自行独立研发获得，并非来自权利人；反向工程，相关信息通过对公开渠道取得的产品开展反向工程分析获得；合法授权，相关信息来自第三方合法授权或许可，具有明确权利来源。

# 第五章 AIGC 企业商业秘密外部保护体系

## 5.1 AIGC 企业商业秘密鉴定

商业秘密鉴定是 AIGC 企业开展维权处置、配合行政监管与司法办案的专业支撑手段。依托专业机构的技术能力与专业知识，针对涉案技术信息与经营信息中的专业问题开展鉴别研判并出具鉴定意见，可为侵权事实认定、损失数额核算、法律责任追究提供依据。

### 5.1.1 商业秘密鉴定的类型

商业秘密鉴定按照实务适用场景与鉴定功能划分三大类型，分别为秘密性鉴定、同一性鉴定、商业秘密侵权损失鉴定，各类型定位清晰且相互配套，覆盖 AIGC 商业秘密维权全流程专业需求。

#### 5.1.1.1 秘密性鉴定

秘密性鉴定是针对权利人主张的技术信息或经营信息开展专业研判，判断相关信息是否满足不为公众所知悉且不易轻易获取，是判定信息能否构成商业秘密的前置核心环节。秘密性认定不以客观上绝对无人知晓为标准，只要落入所属领域人员普遍知悉范畴或是无需付出相应代价即可轻易获取，即不满足秘密性构成要求，包括：相关内容属于行业通用常识或是既定行业惯例，也属于领域内基础开源技术范畴；产品面向市场投放后，外界仅通过外观观测、接口调用即可直接掌握核心技术内容；相关信息已通过学术刊发、行业展会、公开文献等渠道对外披露；社会公众无需投入合理成本，便可从公开途径直接获取同类信息等。

适配 AIGC 行业特点，秘密性鉴定重点围绕模型架构设计、训练数据治理规则、提示词工程策略、模型微调参数配置、算力调度优化逻辑等技术类秘密点展开，同时兼顾客户分层运营、流量转化布局等经营类秘密点，确保鉴定范围全面

覆盖 AIGC 企业核心商业秘密。鉴定过程严格采用多渠道检索、技术横向比对、行业现状研判相结合的方式，全面检索专利文献、学术数据库、预印本平台、代码托管平台、模型与数据集托管平台、开源项目的版本发布说明与提交历史，以及技术博客与开发者社区，细致排查案发时间节点前是否存在同类公开技术。检索时应当将公开状态固定至案发时点，对开源仓库应当核查提交历史时间戳，不以仓库当前内容替代案发时的公开状态；比对行业通用模型框架与竞品技术方案，精准甄别涉案秘密点是否已进入公知领域；引入技术查新成果作为辅助参考，同时严格区分商业秘密秘密性与专利新颖性的认定标准，避免混淆适用。必要时可开展技术勘验、代码审查、模型比对等工作，进一步排除通过常规观测测绘即可获取核心技术的情形，确保鉴定结论的准确性与严谨性。

#### 5.1.1.2 同一性鉴定

同一性鉴定以涉案被控侵权信息与权利人原有商业秘密为核心比对对象，从技术特征、核心要素、关键参数及逻辑架构等多个层面开展综合研判，最终认定二者是否相同或是实质相同，是认定商业秘密侵权行为是否成立的关键依据，直接关系到侵权事实的确认与后续责任的追究。

实质相同的认定遵循统一且明确的标准，若两类信息在核心技术特征、关键运行参数、底层算法逻辑及经营核心策略层面高度重合，仅在非关键表述、格式排版、局部参数微调等方面存在细微差异，且该差异不会改变原有信息的核心功能与商业价值，同时本领域普通技术人员无需创造性劳动即可从一方信息直接导出另一方信息，即可认定为实质相同。

结合 AIGC 领域技术特点，同一性鉴定设置了明确且具体的比对维度，确保比对工作全面、精准。模型层面重点比对网络拓扑结构、激活函数设置、核心模

块布局与权重初始化方式；算法层面聚焦核心代码逻辑、关键功能算子、数据流转流程及安全加密机制；数据层面重点比对训练样本筛选规则、标注标准、脱敏逻辑与特征工程设计；参数层面细致核查超参数配置、学习率调度、正则化设置等关键指标；经营层面则对照用户画像体系、流量转化路径、定价模式及合作渠道核心规则。鉴定过程严格参照行业通用技术规范，采取整体研判与密点逐条比对相结合的方式，明确区分相同、实质相同、相似、不同四种结论，并对实质重合部分作出完整、详细的技术说明，为侵权事实认定提供清晰依据。对于通过反复调用 API 实施模型蒸馏、成员推理、模型逆推的情形，宜以调用日志的分布特征为主要依据、输出结果相似度为辅助依据，开展综合判断。

#### 5.1.1.3 商业秘密侵权损失鉴定

商业秘密侵权损失鉴定以量化侵权行为造成的经济影响为核心目标，针对侵权行为引发的直接损失、侵权获利、合理许可费用、技术价值贬值及维权合理开支等内容，开展专业评估与审计工作，为民事赔偿裁量、刑事入罪标准适用提供精准的量化支撑，是衔接法律责任与经济损失的关键环节。

结合侵权行为的不同发展阶段，损失鉴定适配差异化的鉴定方式，确保鉴定结果贴合实际情况。若仅存在非法获取行为但未投入实际使用，或是侵权产品尚未进入市场流通，即按照同类技术合理许可使用费为基准开展价值评估；若侵权主体已实际使用秘密信息且侵权产品实现市场投放，则通过专业审计方式，精准核算权利人因侵权导致的利润下滑、客户流失等实际损失，同时统计侵权方的产品销量与经营获利数额；若核心秘密信息被公开导致丧失保密属性，则按整体研发投入、技术生命周期收益等指标，测算完整的商业价值损失；针对技术竞争力弱化的情形，单独评估技术贬值额度，而商誉受损则作为实际损失或法定赔偿的

重要考量因素。此外，维权过程中产生的专业服务、公证取证、调查差旅等合理支出，可单独列入鉴定范围并依法主张赔付；若存在恶意侵权且情节严重的情形，可依法主张一至五倍的惩罚性赔偿，进一步加大侵权惩戒力度。

根据损失核算的不同逻辑，需匹配对应资质的鉴定主体。其中，涉及技术价值评估、许可费测算、资产贬值认定的，由具备相应资质的资产评估机构承担；涉及营收核算、利润审计、销量数据核验的，则由具备司法会计资质的专业机构开展专项审计，确保鉴定工作的专业性与合法性。

#### 5.1.2 商业秘密鉴定机构

开展 AIGC 商业秘密鉴定，应当严格依规选择合规专业的鉴定机构，明确机构准入范围、选取标准与委托运行程序，切实保障鉴定意见的合法性、专业性与可信度，确保其能够适配行政执法、民事争议解决与刑事办案等各类场景的需求，为商业秘密保护提供坚实的机构支撑。

##### 5.1.2.1 机构资质与名录

可承接 AIGC 商业秘密司法鉴定及技术鉴定业务的专业机构，实行严格的资质准入管理，对机构执业类型、业务承接范围、专业技术能力、从业人员资质及备案条件均设置明确规范要求。企业在开展 AIGC 商业秘密维权、纠纷处置、侵权取证及司法诉讼相关工作时，可通过官方权威渠道查询经备案、具备合法执业资格的合规鉴定机构名录，择优选择具备相应专业能力和业务资质的机构委托开展鉴定工作。

可查询鉴定机构名录的权威渠道如下：

（1）人民法院委托鉴定系统（dwwtjd.court.gov.cn）；

（2）人民法院诉讼资产网（https://www.rmfysszc.gov.cn）；

（3）国家知识产权局网站（https://www.cnipa.gov.cn）；

（4）中国知识产权研究会官网（www.cnips.org.cn）（行业自律组织推荐名录）。

#### 5.1.2.2 选取标准

企业选取鉴定机构时，应当综合核查多项硬性条件，确保机构能够满足AIGC商业秘密鉴定的专业需求。机构须具备独立法人主体资格，拥有固定的办公场地与专业的技术检测实验室，为鉴定工作开展提供基础保障；从业人员须具备人工智能、计算机算法、大数据研发等相关专业背景，熟悉AIGC模型研发、代码审核与数据安全管控业务，具备足够的专业能力应对复杂的鉴定工作；机构须具备多年知识产权鉴定从业经验，拥有商业秘密相关的鉴定实操案例，且无违规执业、虚假鉴定等不良记录，确保鉴定工作的规范性与可信度；同时，机构需建立完善的内部保密管控机制，严格落实信息权限隔离、操作全程留痕、涉密载体规范处置等管理制度，从业人员需严格履行保密义务，严防鉴定过程中出现商业秘密泄露；此外，机构还需通过行业计量检测、实验室能力认可等相关资质认证，具备规范的鉴定作业流程，保障鉴定工作的标准化开展。

### 5.2 AIGC企业商业秘密保护途径

#### 5.2.1 行政途径

行政途径是AIGC企业商业秘密保护的高效前端渠道，依托市场监督管理部门的执法权力，可快速制止侵权行为、降低维权成本，适用于侵权行为初发、需及时遏制损失蔓延的场景。

#### 5.2.1.1 查处部门与管辖

市场监督管理部门是侵犯商业秘密行为的法定查处部门。国家市场监督管理

总局负责组织、指导全国商业秘密行政保护工作；县级以上地方市场监督管理部门负责本行政区域内商业秘密行政保护工作。[9]

侵犯商业秘密行为一般由违法行为发生地的县级以上市场监督管理部门管辖。[10]技术秘密案件一般由设区的市级以上市场监督管理部门管辖；根据工作需要，经国家市场监督管理总局同意，也可以由具有相应执法能力的县级市场监督管理部门管辖。[11]涉及重大、复杂、跨区域或者有较大社会影响的侵犯商业秘密案件，可以按照市场监督管理行政处罚程序相关规定，由上级市场监督管理部门直接查处或者指定管辖。[12]

#### 5.2.1.2 立案与举报

权利人认为其商业秘密受到侵犯的，可以向市场监督管理部门举报。权利人举报时，应当提供其商业信息属于商业秘密的初步证据材料以及该商业秘密涉嫌被侵犯的具体线索，并对举报内容的真实性负责。市场监督管理部门根据工作需要，可以要求举报人补充举报材料。任何组织和个人不得捏造侵犯商业秘密的事实诬陷他人、实施敲诈勒索，不得滥用举报权利扰乱市场竞争秩序和市场监督管理秩序。[13]权利人可通过三种渠道举报：一是实名注册登录全国12315平台举报；二是拨打北京市场监管投诉举报热线或市民热线举报；三是直接向辖区市场监督管理部门举报。

市场监督管理部门收到举报线索后，应当依法在规定期限内进行核查，由市场监督管理部门负责人决定是否立案；特殊情况下，经市场监督管理部门负责人

[9] 《商业秘密保护规定》第三条。
[10] 《市场监督管理行政处罚程序规定（2022修正）》第七条。
[11] 《商业秘密保护规定》第三条。
[12] 《市场监督管理行政处罚程序规定（2022修正）》第十五条。
[13] 《商业秘密保护规定》第十七条。

批准，可以依法延长核查期限，鉴定等所需时间不计入核查期限。[14]符合“有证据初步证明存在侵犯商业秘密的行为并依法应当给予行政处罚、属于本部门管辖、在给予行政处罚的法定期限内”条件的，应当立案。[15]

#### 5.2.1.3 调查与行政处罚

市场监督管理部门调查侵犯商业秘密案件时，可以依法采取现场检查、询问有关单位或个人、查阅复制有关资料、查封扣押涉案财物、查询银行账户等措施，采取相关措施时，应当符合相关程序规定要求；涉及专门性事项的，当事人可委托法定资质鉴定机构进行鉴定，市场监督管理部门审查后决定是否采纳鉴定结论。

经查证构成侵犯商业秘密的，由市场监督管理部门依据《中华人民共和国反不正当竞争法》的相关规定，责令停止违法行为、没收违法所得，并处以相应罚款，[16]情节严重，符合严重违法失信名单列入条件的，市场监督管理部门可以依照《市场监督管理严重违法失信名单管理办法》作出将当事人列入严重违法失信名单的决定，通过国家企业信用信息公示系统公示，并实施相应管理措施。[17]

市场监督管理部门在作出行政处罚决定时，应当对是否列入严重违法失信名单作出决定。作出列入决定的，应当制作列入严重违法失信名单决定书，载明事由、依据、惩戒措施提示、移出条件和程序以及救济措施等内容。[18]当事人对市场监督管理部门作出的行政处罚决定或者列入严重违法失信名单决定不服的，可依法申请行政复议或提起行政诉讼。

侵犯商业秘密行为涉嫌犯罪的，市场监督管理部门应当依法移送司法机关追

---

14 《市场监督管理行政处罚程序规定（2022 修正）》第十八条。
15 《商业秘密保护规定》第十九条，《市场监督管理行政处罚程序规定（2022 修正）》第十九条。
16 《中华人民共和国反不正当竞争法（2025 修订）》第二十六条，《商业秘密保护规定》第二十四条。
17 《市场监督管理严重违法失信名单管理办法》第二条，第九条第一项。
18 《市场监督管理严重违法失信名单管理办法》第十三条。

究刑事责任，已给予罚款的，折抵相应罚金。

#### 5.2.2 民事途径

民事途径是AIGC企业商业秘密维权的核心救济方式，聚焦权利确认与经济损失弥补，核心围绕当事人主体资格、主管管辖、诉讼要点、证据准备等关键环节开展。

##### 5.2.2.1 当事人主体资格

在侵害商业秘密纠纷案件中，能够举证证明其为商业秘密的权利人或者利害关系人的，可以依法提起侵犯商业秘密诉讼；商业秘密的利害关系人一般是指商业秘密许可合同的被许可人，具体包括：独占使用许可合同的被许可人、排他使用许可合同的被许可人、普通使用许可合同的被许可人。

（1）商业秘密独占使用许可合同的被许可人可单独作为原告起诉；

（2）排他使用许可合同的被许可人可与权利人共同起诉，或在权利人不起诉时自行起诉；

（3）普通使用许可合同的被许可人可与权利人共同起诉，或经权利人书面授权后单独起诉。

##### 5.2.2.2 主管与管辖

侵害商业秘密案件属于侵权之诉，依法由侵权行为地或被告住所地人民法院管辖。[19]侵权行为地包括侵权行为实施地、侵权结果发生地。[20]侵权结果发生地一般为侵权行为直接产生后果的发生地。

北京市辖区内侵犯商业秘密民事纠纷的一审案件，涉及技术秘密的，由北京知识产权法院管辖；涉及经营信息或其他商业信息的，由受理知识产权案件的基

[19] 《中华人民共和国民事诉讼法》第二十九条。

[20] 《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（2022修正）》第二十四条。

层法院管辖；既涉及技术信息又涉及经营信息、其他商业信息的，由北京知识产权法院管辖。当事人对基层法院作出的第一审侵犯商业秘密民事案件的判决、裁定提起的上诉案件，由北京知识产权法院管辖。[21]

#### 5.2.2.3 证据准备

在侵害商业秘密民事诉讼中，原告应当就其享有的商业秘密及被诉侵权行为承担举证责任，提交权利证据、商业秘密构成要件证据及侵权证据。原告提供初步证据，证明其已经对所主张的商业秘密采取保密措施，且合理表明商业秘密被侵犯的，被告应当证明原告所主张的商业秘密不属于法律规定的商业秘密。原告提供初步证据合理表明商业秘密被侵犯，且提供下列证据之一的，被告应当证明其不存在侵犯商业秘密的行为：（一）有证据表明被告有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同；（二）有证据表明商业秘密已经被被告披露、使用或者有被披露、使用的风险；（三）有其他证据表明商业秘密被被告侵犯。诉讼过程中，当事人可申请不公开审理、限制涉密证据接触人员范围、明确涉密证据开示方式，防止秘密点进一步泄露。此外，证据可能灭失或难以取得时，可申请法院进行证据保全。

### 5.2.3 刑事途径

刑事途径是 AIGC 企业商业秘密保护中惩戒力度较强的救济方式，主要适用于行为人以盗窃、贿赂、欺诈、胁迫、电子侵入、非法复制等不正当手段获取商业秘密，或者违反保密义务、违反权利人有关保守商业秘密的要求，披露、使用、允许他人使用商业秘密，并达到刑事追诉标准的情形。对于核心商业秘密被非法获取、披露或者使用，造成重大损害或者存在严重危害后果的，AIGC 企业

[21] 《北京知识产权法院侵犯商业秘密民事案件当事人诉讼问题解答》（2023 年）第五部分程序事项，第 37 条。

可以依法向公安机关报案，请求追究行为人的刑事责任。

#### 5.2.3.1 罪名与行为类型

侵犯商业秘密行为达到刑事追诉标准的，可能构成《中华人民共和国刑法》第二百一十九条规定的侵犯商业秘密罪。根据该条规定，侵犯商业秘密的主要行为包括：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；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；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；明知前述行为，获取、披露、使用或者允许他人使用该商业秘密的行为。[22]

结合相关司法解释及 AIGC 行业特点，行为人通过非法复制模型文件、训练数据、源代码、项目文档等方式获取商业秘密的，可以认定为刑法第二百一十九条第一款第一项规定的“盗窃”；未经授权或者超越授权使用计算机信息系统、代码仓库、模型训练平台、数据管理系统、云服务后台等方式获取商业秘密的，可以认定为“电子侵入”。[23]

为境外机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，还可能构成为境外窃取、刺探、收买、非法提供商业秘密罪。[24]AIGC 企业在跨境研发、境外外包、海外云服务、国际技术合作、境外融资或者业务出海过程中，应特别关注核心商业秘密被非法向境外提供的刑事风险。

#### 5.2.3.2 管辖规则

侵犯商业秘密犯罪案件由犯罪地公安机关立案侦查。必要时，可以由犯罪嫌

---

22 《中华人民共和国刑法修正案（十一）》第二十二条。

23《最高人民法院　最高人民检察院关于办理侵犯知识产权刑事案件适用法律若干问题的解释》第十六条。

24 《中华人民共和国刑法修正案（十一）》第二十三条。

疑人居住地公安机关立案侦查。侵犯商业秘密犯罪案件的犯罪地，包括侵权产品制造地、储存地、运输地、销售地，传播侵权作品、销售侵权产品的网站服务器所在地、网络接入地、网站建立者或者管理者所在地，侵权作品上传者所在地，权利人受到实际侵害的犯罪结果发生地。对有多个侵犯商业秘密犯罪地的，由最初受理的公安机关或者主要犯罪地公安机关管辖。多个侵犯商业秘密犯罪地的公安机关对管辖有争议的，由共同的上级公安机关指定管辖，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的同级人民检察院、人民法院受理。

对于不同犯罪嫌疑人、犯罪团伙跨地区实施的涉及同一批侵权产品的制造、储存、运输、销售等侵犯商业秘密犯罪行为，符合并案处理要求的，有关公安机关可以一并立案侦查，需要提请批准逮捕、移送审查起诉、提起公诉的，由该公安机关所在地的同级人民检察院、人民法院受理。[25]

#### 5.2.3.3 立案追诉与量刑升档标准

侵犯商业秘密，具有下列情形之一的，应当认定为刑法第二百一十九条规定的“情节严重”，依法予以刑事追诉：[26]

（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）二年内因实施刑法第二百一十九条、第二百一十九条之一规定的行为受过刑事处罚或者行政处罚后再次实施，造成损失数额或者违法所得数额在十万元以上的；

---

[25] 《关于办理侵犯知识产权刑事案件适用法律若干问题的意见》第一条。

[26]《最高人民法院　最高人民检察院关于办理侵犯知识产权刑事案件适用法律若干问题的解释》第十七条，《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》。

（4）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；

（5）其他给商业秘密权利人造成重大损失的情形。

侵犯商业秘密，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，或者数额达到本条前款相应规定标准十倍以上的，应当认定为刑法第二百一十九条规定的“情节特别严重”。

涉及为境外机构、组织、人员窃取、刺探、收买、非法提供商业秘密的刑事风险，参见本指引第六章“海外保护”相关内容。

#### 5.2.3.4 损失数额与违法所得数额认定

损失数额与违法所得数额，是判断侵犯商业秘密行为是否达到刑事追诉标准、是否构成“情节严重”或者“情节特别严重”的重要依据。AIGC 企业在启动刑事报案前，可结合侵权行为类型、商业秘密性质、泄露范围、实际使用情况及危害后果，对损失数额或者违法所得数额进行初步测算，并同步准备研发投入、商业化收益、许可交易、侵权产品或者服务收入、客户流失、补救费用等相关证明材料。

侵犯商业秘密刑事案件中的损失数额，可以按照以下路径认定：[27]

（1）侵入型、窃取型侵权的损失计算。行为人以盗窃、非法复制、电子侵入或者其他不正当手段获取商业秘密，尚未披露、使用或者允许他人使用的，损失数额可以根据该项商业秘密的合理许可使用费确定。此类情形下，刑事追诉并不当然要求权利人证明行为人已经实际使用商业秘密。对于 AIGC 企业而言，非法下载模型权重、复制源代码、越权进入训练平台、导出训练数据集、窃取提示词库或者工作流配置等行为，即使尚未形成对外销售产品或者服务，也可以围

[27]《最高人民法院 最高人民检察院关于办理侵犯知识产权刑事案件适用法律若干问题的解释》第十八条。

绕合理许可使用费、技术授权价值、同类项目报价、开发替代成本等材料开展损失测算。

（2）违约型、使用型侵权的损失计算。行为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，披露、使用或者允许他人使用其所掌握的商业秘密的，损失数额可以根据权利人因被侵权造成的利润损失确定。行为人以不正当手段获取商业秘密后又披露、使用或者允许他人使用，或者明知相关商业秘密来源非法仍获取、披露、使用或者允许他人使用的，也可以根据权利人的利润损失确定；利润损失低于该项商业秘密合理许可使用费的，可以根据合理许可使用费确定。权利人利润损失可以结合客户、项目流失，产品或者服务收入减少，模型调用收入下降，SaaS 订阅收入下降，API 服务收入减少，内容制作项目减少等情况进行测算；无法直接确定销售量或者服务量减少的，可以结合侵权产品销售量、侵权服务收入、平台流水、合同金额、用户付费记录等材料进行辅助核算。

（3）商业秘密丧失秘密性或者灭失的损失计算。因侵犯商业秘密行为导致商业秘密已为公众所知悉或者灭失的，损失数额可以根据该项商业秘密的商业价值确定。商业价值可以综合研究开发成本、实施收益等因素评估。对于 AIGC 核心商业秘密而言，一旦被公开传播、上传至公开平台、被多主体获取或者被同行复用，可能导致秘密性基础受损，企业可以围绕该项秘密整体商业价值主张损失。

#### 5.2.3.5 公诉与自诉程序

针对侵犯商业秘密犯罪行为符合立案标准的，权利人可直接向公安机关报案，由侦查机关立案侦办，依法追究涉案人员的刑事法律责任。若权利人有充分证据证明侵犯商业秘密行为理应追究刑事责任、但人民检察院没有提起公诉的，

权利人可直接向人民法院提起刑事自诉。[28]

### 5.3 AIGC 企业商业秘密保护路径选择与衔接

AIGC 企业遭遇商业秘密侵权时，可以根据侵权行为性质、证据掌握程度、损失规模、紧急程度及维权目标，综合选择行政、民事、刑事等保护途径。行政途径侧重快速制止侵权、固定初步证据，并可依法降低举证难度；民事途径侧重确认权利边界、追究侵权责任和弥补经济损失；刑事途径侧重打击情节严重、危害较大的侵犯商业秘密行为。三种途径并非固定先后关系，企业应结合具体案件情况灵活决策，并做好程序之间的证据衔接和维权协同。

对于侵权行为较为明确、侵权仍在持续、企业主要目标是快速止损和控制扩散的，可以优先考虑行政投诉；对于损失数额或者违法所得数额已达到刑事追诉标准，或者存在证据灭失风险的，可以直接向公安机关报案；对于需要确认权利归属、主张停止侵害、赔偿损失、消除影响或者解决民事法律关系衍生争议的，可以依法提起民事诉讼或者仲裁。企业也可以根据案件进展，在行政查处、民事诉讼和刑事追责之间进行有效衔接，形成多层次保护。

#### 5.3.1 行政途径与民事、刑事程序的衔接

企业通过行政途径维权的，应在提交举报材料时同步考虑后续民事诉讼或者刑事追责需要，围绕商业秘密构成要件、保密措施、侵权行为、同一性比对、损失后果等内容准备证据。行政查处过程中形成的证据材料，可以依法在后续民事诉讼或者刑事追责中使用。行政查处过程中，如发现侵权行为涉嫌犯罪，行政机关可以依法移送司法机关处理。企业也应同步关注损失数额、违法所得数额、重复侵权、恶意窃取核心技术、证据灭失等情形，必要时及时向公安机关报案，避

[28] 《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》第一条。

免因程序选择不当影响取证和追责。

### 5.3.2 民事途径与行政、刑事程序的衔接

企业通过民事途径维权的，可以结合案件需要，申请证据保全、行为保全、财产保全，并申请法院对涉密证据采取保密措施。已经通过行政查处或者刑事程序固定的证据，可以依法在民事程序中使用。对于侵权行为虽未达到刑事追诉标准，但已经造成经济损失的，企业可以通过民事诉讼主张停止侵害、赔偿损失、赔偿维权合理开支等责任。对于恶意侵犯商业秘密且情节严重的，可以依法主张惩罚性赔偿。

### 5.3.3 刑事途径与民事、行政程序的衔接

刑事途径适用于侵犯商业秘密行为情节严重、损失数额或者违法所得数额达到刑事追诉标准，或者行为人具有明显非法获取、披露、使用商业秘密意图，且存在证据灭失、继续扩散、人员潜逃、设备转移等紧急风险的情形。对于内部人员、离职员工、核心研发人员、合作方人员非法复制模型权重、训练数据、源代码、提示词库、客户资料等核心商业秘密，或者通过电子侵入、越权访问、批量下载、私自外传等方式获取商业秘密的，达到刑事追诉标准的，企业可以直接向公安机关报案。刑事程序并不排除企业依法主张民事赔偿。企业可以根据案件情况，提起刑事附带民事诉讼。对于尚不足以追究刑责但存在违法或者侵权事实的，也可以根据案件情况转向行政投诉或者民事诉讼，持续维护自身权益。

## 第六章 AIGC 企业商业秘密海外保护

### 6.1AIGC 企业面临的主要风险场景

### 6.1.1 数据管理与技术环境风险

（1）数据跨境传输泄露风险。AIGC 企业在开展跨境业务、模型联合训练、

境外业务布局过程中，涉及训练数据集、模型参数、提示词库等核心商业秘密跨境流转。若未落实加密、脱敏、分级管控等安全防护举措，相关涉密信息在跨境传输链路中易被截取，造成无形技术秘密外泄。

（2）境外云服务与通用 AI 工具使用风险。企业选用海外云服务商存储、部署 AIGC 模型及业务数据时，容易因平台配置疏漏、权限开放不当，引发涉密模型与经营数据对外公开。员工日常办公若随意将包含模型架构、算法思路、业务方案等涉密内容输入境外通用人工智能工具，相关信息可能被纳入模型训练素材，造成商业秘密被动留存与扩散。部分企业通过第三方中转、代理接入等方式使用境外模型服务的，相关提示词、业务数据与技术方案需经中转服务方处理转发，同样存在被留存、复用与外泄的风险。

（3）跨境远程办公安全隐患。企业研发、运营人员在境外开展工作，使用个人终端设备接入企业内网处理 AIGC 涉密业务时，受设备安全防护缺失、公共网络环境不可控等因素影响，极易出现模型资料、训练数据等外泄情形。

### 6.1.2 外部渗透与同业竞争风险

（1）商业间谍与网络窃取风险。行业境外竞争对手可通过拉拢企业核心技术人员或雇佣专业网络攻击力量等方式，入侵企业研发系统与数据平台，非法窃取 AIGC 模型架构、算法逻辑、定制化训练方案等核心商业秘密，形成不正当竞争优势。

（2）海外供应链合作渗透风险。AIGC 企业在境外数据标注、算力外包、产业合作等供应链环节中，若合作第三方内部管理不规范，网络防护薄弱，极易被外部势力渗透利用。合作过程中向境外合作方提供的模型资料、技术接口、业务规则等涉密信息，存在不当外流的现实风险。

#### 6.1.3 跨境交易与知识产权纠纷风险

（1）跨境技术合作与授权交易风险。企业在海外开展 AIGC 技术许可、项目联合研发等商事活动时，若合作协议权利义务约定模糊、保密约束不完善，合作方可能超范围使用模型技术，擅自向第三方披露、转让相关商业秘密，侵害企业合法权益。

（2）跨境知识产权涉诉衍生风险。AIGC 企业在海外遭遇商业秘密侵权指控或发起维权诉讼过程中，需要提交模型秘密点、研发过程、技术比对等涉密材料作为证据。若未设置专门保密程序与信息隔离机制，诉讼举证环节易引发核心商业秘密二次扩散。

### 6.2 AIGC 企业的应对策略

#### 6.2.1 完善跨境合作制度与合同约束

（1）规范海外供应链保密约定。与境外数据标注、算力服务及技术外包等合作主体签订专项保密条款，明确涉密范围、保密义务、违约责任及高额惩戒标准，同时约定技术资料、模型文档的使用期限与留存要求，到期必须全部销毁，不得私自备份留存。

（2）细化跨境合资与研发协议。在境外合资和联合研发合作文本中，清晰界定 AIGC 模型、算法、训练数据等知识产权权属，设置分阶段分层级技术披露机制，严控核心秘密点对外公开范围，杜绝无边界技术共享带来的泄密风险。

#### 6.2.2 强化全流程技术安全防控

（1）严格管控核心数据跨境出境。企业优先选用合规可控的国内加密云平台存储 AIGC 核心模型、原始训练数据等涉密资产；确需向境外传输业务资料的，事前做好脱敏脱密处理。对图像、音频、视频类资料，可嵌入隐形数字水印；对

文档、代码、数据集等文本类资料，宜按接收方分版交付（不同接收方对应不同可识别标记），并配合交付内容哈希登记来实现溯源，不宜依赖文本隐形水印。

（2）健全境外访问与操作监控。部署企业内网安全管控体系，对境外人员访问模型系统、调取涉密文档等行为实施实时监测、异常预警。境外办公终端统一安装数据防泄露管控程序，严格限制私自外接存储设备、违规跨平台上传涉密资料等操作行为。

#### 6.2.3 规范外派及跨境人员管理

（1）落实核心岗位跨境管控机制。对赴境外开展研发、技术对接的核心岗位人员，推行关键操作双人复核、共同授权制度，避免单人独立接触、处置 AIGC 核心商业秘密，降低人为泄露风险。

（2）完善外派人员合约与离境审计。在外派劳动合同及保密协议中，增设跨境履职、归国离岗专项约束条款。人员结束境外工作归国前，统一开展办公设备检查、涉密数据清理、工作文档封存，杜绝私自留存、带走模型资料与涉密信息。

## 第七章 附则

### 7.1 指引的解释

本指引由北京市市场监督管理局负责解释。

### 7.2 施行日期

本指引自发布之日起施行。