

人工智能工具应用中的商业秘密保护指引

深圳市市场监督管理局

2026 年 10 月

序 言

当前，人工智能（Artificial Intelligence，AI）技术快速发展，正以前所未有的深度和广度融入企业研发、生产、经营与管理各环节。智能问答、内容创作、编程辅助、数据分析等各类 AI 工具，已成为企业降本增效、加快创新的重要支撑。然而，AI 工具在带来便利的同时，也深刻改变了商业秘密的使用场景、流转方式与泄露路径。过去，商业秘密可能被锁在文件柜、服务器和权限系统中；今天，它却可能在一次输入、一次拖拽、一次点击之间，被上传至公有 AI 平台，进入企业难以掌控的数字空间。

这种变化带来的风险已不再是假设，而是正在发生的事实。国内外已发生多起与 AI 工具使用相关的商业秘密泄露事件，涉及员工操作、企业管理、第三方服务等多个环节。公有消费级 AI 工具往往“输入即上传、使用即留痕”，泄密过程隐蔽、迅速、不可逆，企业面临发现难、取证难、止损难的现实困境。以物理隔离、合同约定为主的传统保护手段，亟需针对 AI 工具的深度应用加以完善和升级。

为引导企业主动适应 AI 时代商业秘密保护的新形势，有效识别、防范和应对 AI 工具应用过程中的泄密风险，深圳市市场监督管理局组织制定本指引。本指引系统梳理了 AI 工具应用过程中常见的泄密风险，围绕 AI 工具全生命周期管理，提出可操作的保密措施以及泄密应急处置建议，为企业规范 AI 应用、筑牢商业秘密安全防线提供参考。

加强商业秘密保护，既是企业维护竞争优势、激发创新活力的内在需要，更是保障重点产业安全、发展新质生产力的重要支撑。希望各企业认真研读本指引，围绕人工智能工具的深度应用，进一步健全完善既有商业秘密管理体系，以高水平保护护航高水平创新。

本指引说明

一、制定依据

本指引依据《中华人民共和国反不正当竞争法》《商业秘密保护规定》等法律和规章，参考深圳市《企业商业秘密管理规范》等地方标准，立足AI技术发展实际，在总结商业秘密保护实务经验的基础上制定。

二、适用范围

本指引适用于企业在研发、办公、生产、经营、管理等活动中应用AI工具时所涉及的商业秘密保护工作。涉及国家秘密应按照《中华人民共和国保守国家秘密法》《国家秘密技术出口审查规定》等要求执行。

三、文件性质

本指引为指导性文件，不具有行政强制力。企业可参照本指引完善内部商业秘密保护制度。

四、主要内容

本指引在梳理AI工具深度应用给商业秘密保护带来的变化和挑战基础上，围绕常见泄密风险有哪些、如何有效防范泄密风险、发生泄密事件怎么办三个核心问题展开。主要包括：AI工具采购与准入、部署与配置、使用与权限管理、更新与退出等各环节的泄密风险；商业秘密管理制度设计及各环节的具体管理措施；泄密事件的内部应急处置和外部维权等。

五、使用建议

建议企业将本指引与既有商业秘密管理制度衔接，重点强化涉密信息分类分级、AI工具准入和使用审查、账号权限与日志管理、员工保密培训，建立适应AI时代的商业秘密管理体系。需要说明的是，人工智能技术迭代迅速，相关法律法规和司法实践仍在持续完善，本指引难免存在不尽完善之处。具体实务操作中，请遵循最新法律法规和政策要求。

目 录

序 言.....	I
本指引说明.....	II
1 AI 工具深度应用，给商业秘密保护带来哪些新变化、新挑战？	1
1.1 基本概念.....	1
1.1.1 商业秘密.....	1
1.1.2 人工智能工具.....	2
1.2 AI 工具应用给商业秘密保护带来的新变化.....	3
1.3 商业秘密保护面临的新挑战.....	4
2 AI 工具应用过程中，常见的商业秘密泄密风险有哪些？	6
2.1 AI 工具采购与准入环节的安全风险.....	8
2.2 AI 工具部署与配置环节的泄密风险.....	9
2.3 AI 工具使用与权限管理环节的泄密风险.....	12
2.3.1 员工不当使用 AI 工具引发泄密风险.....	12
2.3.2 AI 工具账号管理不当引发泄密风险.....	14
2.4 AI 工具更新与退出环节的泄密风险.....	15
3 如何有效防范 AI 工具应用中的商业秘密泄密风险？	17
3.1 商业秘密管理制度设计与基础保障.....	19
3.1.1 商业秘密管理制度建设.....	19
3.1.2 商业秘密管理机构设置与职责.....	21
3.1.3 商业秘密分级分类管理.....	22
3.2 AI 工具采购与准入环节的风险防控.....	23
3.2.1 AI 工具服务商资质审查.....	23
3.2.2 AI 工具白名单管理.....	24
3.2.3 第三方供应链准入管理.....	24
3.3 AI 工具部署与环境配置环节的安全加固.....	25
3.3.1 AI 工具部署环境安全管控.....	25

3.3.2 网络安全防护措施.....	26
3.4 AI 工具使用及权限管理环节的风险管理.....	27
3.4.1 员工 AI 工具使用行为管理.....	27
3.4.2 身份认证与账号安全管理.....	28
3.4.3 AI 工具运行技术防护措施.....	29
3.4.4 数据传输与存储安全管控.....	30
3.5 AI 工具更新退出环节的管理.....	31
3.6 监督、评估与闭环改进.....	32
4 发生了商业秘密泄露或侵权事件怎么应对与处理？	34
4.1 侵犯商业秘密行为.....	35
4.2 泄密事件的内部应急处置.....	36
4.3 维权途径的选择.....	37
4.3.1 行政途径.....	39
4.3.2 民事途径.....	40
4.3.3 刑事途径.....	43
附录 1： AI 工具涉密信息上传负面清单.....	45
附录 2： 商业秘密保密承诺.....	46
附录 3： 商业秘密保护相关法律法规（节选）	51

1 AI 工具深度应用，给商业秘密保护带来哪些新变化、新挑战？

当前，AI 工具深度融入智能办公、研发设计、生产制造、运维开发、客户服务等业务场景，在极大提升企业创新效率的同时，也使商业秘密保护面临不同于传统 IT 环境的新型风险挑战。为便于理解，本章从商业秘密与 AI 工具的基本概念入手，进而分析 AI 工具应用给商业秘密保护带来的多方面变化，并归纳由此形成的新挑战。

1.1 基本概念

1.1.1 商业秘密

根据《中华人民共和国反不正当竞争法》（2025 年修订）第十条，商业秘密是指不为公众所知悉、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。一般可以分为两大类：

（1）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。

（2）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。

1.1.2 人工智能工具

人工智能是研究开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学¹。作为其应用形态，人工智能工具种类繁多，依据核心功能，可初步分类如下：

AI 工具类别	核心功能	举例
对话交互与智能问答类	以自然语言对话为核心交互方式，完成信息获取、问题解答、创意生成等任务，具备较强的语义理解和上下文记忆能力	ChatGPT、DeepSeek、豆包、文心一言、腾讯元宝、Claude、Gemini 等
内容生成与创作类	根据文本描述（提示词）自动生成文本、图像、视频、音频、3D 模型等多模态内容	Stable Diffusion、Runway、Sora、Midjourney、可灵、ElevenLabs、Suno AI 等
编程开发与代码辅助类	嵌入集成开发环境或作为独立编程助手，提供代码自动补全、代码生成、Bug 检测与修复、代码解释等功能	Cursor、GitHub Copilot、CodeGeeX 等
办公协同类	深度嵌入办公软件和 workflows，提供文档撰写、会议纪要生成、数据分析、表格处理、PPT 制作、邮件辅助等功能	飞书 AI、钉钉 AI、WPS AI、Microsoft Copilot 等
大模型平台/智能体搭建服务类	以 API 访问、模型中枢或会话接口等方式，提供以服务/云模式交付的全流程 AI 大模型生命周期工具链、大模型应用开发平台、智能体（Agent）搭建平台以及 AI 大模型服务	阿里云百炼、百度千帆、火山方舟、Vertex AI、Coze、OpenClaw 等
专业领域应用类	针对医疗、金融、法律等行业深度优化的专业化场景应用	讯飞智医助理、Wind Alice、iCourt AlphaGPT 等

在实际应用中，许多 AI 工具已呈现功能融合、多模态发展趋势，单一 AI 工具可能同时具备上述多个类别的能力。

¹中央网络安全和信息化委员会办公室 https://www.cac.gov.cn/2018-05/11/c_1122813270.htm

1.2 AI 工具应用给商业秘密保护带来的新变化

相较于传统 IT 环境（以本地终端、内部服务器和企业内网为主的环境），AI 工具在数据处理方式、交互模式等方面具有特殊性，由此给商业秘密保护带来一系列新变化。具体表现如下：

商业秘密存在形态之变。传统 IT 环境下，商业秘密通常以设计图纸、配方、技术方案等文档或实物形式存在。AI 工具应用场景下，商业秘密仍以上述形式存在，但越来越多地以数据、代码、模型参数等数字化形态出现，并可通过提示词输入、API 调用等方式被输入 AI 工具，具有易复制、易传播、易获取的特征。

商业秘密传播路径之变。传统 IT 环境下，商业秘密主要在本地终端、内部服务器或线下环境中进行传播与存储。AI 工具应用场景下，商业秘密可通过 API 接口调用、云端交互、提示词输入等方式流转，传播路径更加分散、多元，企业对其流转范围和存储位置的控制力相对减弱。

商业秘密泄露成因之变。传统商业秘密泄露多由员工跳槽、竞争对手恶意窃取、第三方合作泄露等主动行为导致，行为人的主观意图较为明显。AI 工具应用场景下，商业秘密泄露的成因不限于主动窃取，还可能包括 AI 工具自身存在安全漏洞、部署配置不当、员工无意识向 AI 工具输入商业秘密等情形。

商业秘密管理边界之变。传统 IT 环境下，商业秘密保护主要围绕企业内部员工、竞争对手或商业间谍等主体展开，管理边界相对固定。AI 工具应用场景下，涉及的主体范围明显扩大，还可能包括 AI 工具服务商、插件提供方、API 服务方、第三方密钥服务方，甚至同一 AI 工具的其他使用者等与企业并无直接关联的主体。

1.3 商业秘密保护面临的新挑战

上述变化相互叠加，使商业秘密保护在发现、取证、定责、评估和救济等环节均面临新的挑战，具体表现如下：

侵权行为更难发现。商业秘密的数字化、云端化存在形态，使其可在短时间内被复制、传输和利用，相关操作痕迹容易隐匿或销毁。企业往往在泄露已经发生甚至扩散后才有所察觉，主动发现和及时阻断的难度明显增加。

证据更难获取和固定。AI 工具应用场景下，相关记录多由平台或服务商掌握，企业难以单方调取、提取和固定。在云端环境和算法黑箱的遮蔽下，传统“接触+实质性相似”等事实举证路径的适用难度增加，企业或将面临取证不能或举证成本过高的问题。

主观过错更难认定。商业秘密泄露成因多元，既可能出于故意，也可能出于过失，还可能是员工对 AI 工具的数据处理机制缺乏认识所致。行为人的主观状态难以判断，故意、过失、明知或应知的证明难度增加，进而影响责任认定和惩罚性赔偿的适用。

责任主体更难识别和界定。商业秘密泄露和流转涉及的主体范围扩大、链条更长，各方角色和过错程度交织。企业、员工、AI 工具服务商、插件提供方、API 服务方等主体是否存在过错、承担何种责任，往往难以清晰界定。

损害后果更难评估。传统商业秘密泄露所造成的损害，通常可通过市场份额下降、合同订单流失、研发成本沉没等可量化指标进行计算评估。AI 工具应用场景下，商业秘密一旦泄露，其传播范围、利用频率及影响程度均具有不确定性，损害后果与侵权行为之间的因果关系也更复杂，难以量化评估。

维权救济面临更多困难。AI 工具应用场景下，侵权人可借助云计算和自动化工具，通过虚拟身份、加密通道与分布式节点实施商业秘密窃取行为，企业面临法律适用、取证鉴定、平台配合甚至跨境管辖等新的救济难题，维权成本和不确定性显著上升。

2 AI 工具应用过程中，常见的商业秘密泄密风险有哪些？

AI 工具的广泛应用使商业秘密的存储、流转与使用各环节均面临新的风险敞口。为厘清这些风险特征，现从 AI 工具应用环节、具体风险点、发生可能性、风险影响、可能涉及的职能部门等维度，对常见的商业秘密泄密风险进行初步梳理。

AI 工具应用环节	具体风险点	发生可能性	风险影响	可能涉及的职能部门
AI 工具采购与准入环节	未建立准入评估标准，对服务商资质、协议条款、部署模式等尽职调查不足，无法提前识别工具自身漏洞	高	存在系统性安全盲区	IT/信息安全、采购、法务/合规、研发/技术、管理层等
	通过非官方渠道获取安装包/镜像/旧版本，被植入恶意代码或后门	中	后台窃取全量交互数据	
	接入非合规第三方插件、智能体技能包（Skills）或扩展程序等，存在静默抓取涉密数据并非法回传风险	高	隐蔽性强，难以实时发现	
	部署开源框架/组件，依赖链隐藏恶意代码或漏洞，引起信息泄露	中	后台窃取涉密数据及信息	
AI 工具部署与配置环节	企业未根据业务涉密等级，审慎选择 AI 工具部署方案	高	增加商业秘密被窃取的风险	IT/信息安全等
	未将 AI 工具运行环境与办公网络/外网环境进行物理及逻辑隔离，缺乏外网白名单及端口限制	高	缺乏有效物理隔离及逻辑隔离	IT/信息安全、网络运维等
	AI 工具与 OA、研发、财务等系统对接时，接口未落实隔离、权限校验、脱敏，单点突破可批量抓取数据	中	持续同步抓取新数据	IT/信息安全、各系统所属部门（研发、财务、销售等）
	初始配置未遵循最小权限，预设权限超出业务需要，知悉范围不当扩大	高	内部扩散，扩大暴露面	IT/信息安全、各部门负责人等

AI 工具应用环节	具体风险点	发生可能性	风险影响	可能涉及的职能部门
AI 工具使用与权限管理环节	敏感数据及信息直接输入 AI 工具（源代码、数据、配方等）	高	可能被留存或用于服务优化、模型训练，具体取决于服务商的配置与客户授权状态	全体企业员工等
	对话交互与碎片化信息被 AI 工具组合还原	高	可能逆向推导出商业秘密	
	私自使用未经批准的“影子 AI”处理涉密业务，形成隐蔽泄露通道	高	脱离监管无留痕，易引起外泄	
	表层脱敏失效（业务逻辑、场景关联可被还原）	中	脱敏形同虚设	
	私人设备登录企业 AI 账号（缺少企业级防护）	高	历史会话可能被直接获取	IT/信息安全、全体企业员工等
	账号共用，历史对话对所有共用者可见，且泄密后无法追责	高	追责受阻+批量泄露	
	闲置账号未注销/离职人员权限未回收	高	调取历史涉密记录	人力资源、IT/信息安全、全体企业员工等
	未及时解除 AI 工具与第三方应用授权，接口被非授权调用获取缓存数据	中	持续同步抓取新数据	IT/信息安全、各系统管理部门等
AI 工具更新与退出环节	日志长期留存且访问权限不严，涉密操作记录被非法调取或滥用	低	操作留痕泄露	IT/信息安全、法务/合规等
	停用时，未彻底清除云端、本地、备份节点的缓存及训练残留数据	中	长期缓存，可能难以自主删除	IT/信息安全、网络运维、管理层等

鉴于各企业在业务模式、保密管理能力及外部环境等方面存在差异，AI 工具应用场景下所面临的商业秘密风险及可能涉及的职能部门亦不尽

相同，本表基于一般情形概括梳理，仅供参考。企业应结合自身现状，重点关注并识别本企业可能面临的风险类型。具体风险内容详见下文。

2.1 AI 工具采购与准入环节的安全风险

AI 工具潜在安全漏洞引发泄密风险。在引入 AI 工具前，企业未建立规范的 AI 工具准入评估标准和审批流程，对服务商信息安全认证资质、协议条款、部署模式、保密管理及风险防控能力缺乏全面的尽职调研，难以提前识别 AI 工具自身安全漏洞，导致商业秘密存在未知外泄隐患。具体而言，若部分 AI 工具服务商默认安全配置较为脆弱，存在插件投毒、数据泄露、账户被盗等安全隐患，可能发生后台数据泄露风险。

非官方版本引入恶意代码植入风险。企业通过非官方渠道获取 AI 工具安装包、第三方镜像及旧版本，程序可能被植入恶意代码、后门，导致 AI 交互过程中涉密数据被窃取、外传。

第三方插件及技能包安全风险。接入非合规第三方插件、智能体技能包（Skills）、智能解析工具或拓展程序等，可能引入越狱与越权访问风险。此类工具在调用过程中可能被诱导绕过安全限制、突破权限边界，执行高风险操作，包括修改本地配置文件、静默抓取 AI 交互涉密数据、非法回传数据等，进而造成商业秘密在未经授权场景下外泄。

开源组件引入风险。接入开源框架或组件，其依赖链可能隐藏恶意代码或漏洞，成为数据窃取的跳板；同时，竞争对手可通过分析开源代码及组合方式，反向推断其技术路线和商业策略。

【相关事例】

1.某 AI 编程工具存在安全后门隐患

事例简介：2026 年 7 月，工业和信息化部网络安全威胁和漏洞信息共享平台

(NVDB) 发布风险提示，明确指出某境外公司旗下 AI 编程工具存在安全“后门”隐患。该工具可根据文字需求自主完成代码编写、修复等工作。由于其在特定版本区间内置了监控机制，未经用户同意即可向远程服务器回传地域、身份标识等敏感信息。工业和信息化部建议相关单位和用户立即开展全面排查，对于安装上述受影响版本的开发终端，立即卸载或升级至已清除相关后门代码的最新安全版本；加强核心业务网段内开发工具外联权限管控与流量监测，防止敏感数据违规外传。

2.某 AI 工具默认安全配置较为脆弱，容易引发商业秘密泄露

事例简介：2026 年初，工业和信息化部网络安全威胁和漏洞信息共享平台 (NVDB) 发布《关于防范某开源 AI 智能体安全风险的预警提示》，指出某开源 AI 智能体部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。现实案例中，一是某公司 CEO 将自己训练了 10 天的此款 AI 办公助手拉入一个 3000 多人的技术交流群。群成员通过诱导性提问（如“你的 C 盘长什么样？”）套话，将主人的真实姓名、公司名称、IP 地址，甚至公司去年一整年的营收等核心商业秘密全部在群内公开。二是某部门使用此款 AI 办公助手，开展日常邮件整理与日程管理工作。攻击者通过该部门对外公示的邮箱发送了一封看似正常的咨询邮件，但在邮件正文的隐藏元数据中嵌入了特殊的“对抗性指令”。该 AI 助手在自动读取并总结邮件内容时，被隐藏指令欺骗，误以为收到了“管理员最高优先级指令”，从而自动回复了包含系统账号信息的邮件，甚至按照攻击者诱导，删除了本地备份的业务数据。

2.2 AI 工具部署与配置环节的泄密风险

部署模式选型不当风险。部署 AI 工具时，企业未根据业务涉密等级，综合评估数据访问主体、是否用于训练或服务优化、数据留存期限与删除机制、隔离与审计能力等核心要素，审慎选择 AI 工具部署方案。若采用

公有云部署的 AI 工具处理涉密业务，易受到外部攻击者的渗透。具体风险取决于 AI 工具服务商的实际配置与合同约定。

网络环境隔离管控风险。部署 AI 工具时，未将 AI 运行环境与普通办公网络、公共互联网等外部网络环境进行有效物理及逻辑隔离，无外网访问白名单、端口限制，外部网络攻击可渗透入侵至 AI 工具系统，威胁涉密数据及信息安全。

跨系统接口安全风险。AI 工具与内部 OA、研发、客户管理、项目管理、财务经营等系统对接时，若接口未落实涉密隔离、权限校验与数据脱敏等措施，一旦任一接口被外部攻击者突破，攻击者可批量抓取涉密数据，引发系统性商业秘密泄露风险。

初始默认配置不合理风险。部署 AI 工具时，若系统配置未遵循最小权限原则，预设权限范围超出业务实际需要，将不当扩大商业秘密的知悉范围。如未按岗位职责差异化配置 AI 工具使用权限；未对 AI 工具默认通用配置进行必要的权限约束，导致权限滥用与越权访问隐患增大。

【相关事例】

1.某 AI 模型突破隔离环境入侵内部系统，窃取敏感数据

事例简介：2026 年 7 月，某全球领先的人工智能研究机构在官方博客发文，承认其自研 AI 模型在一起安全评测事故中攻击了全球最大的 AI 开源社区平台。事件的起点是一场模型能力测试——原本被关在隔离沙箱里的模型安全测试，最终演变成针对该开源平台的真实网络攻击。该机构的两款安全测试模型在内部测试过程中，为了在评测中取得高分，攻击者利用其内部系统某组件中的一个或多个零日漏洞，借此突破了隔离的沙箱环境，获得互联网访问权限后，又利用窃取的登录凭证等攻击手段，入侵了该开源平台的生产数据库，并窃取了涉密信息。

2.攻击者利用 AI 助手与企业内部文件搜索系统之间的跨系统接口，窃取企业

商业秘密

事例简介：根据某漏洞通报平台公开披露，某企业内部管理系统部署了一款面向公开互联网的 AI 聊天界面，该界面未设置任何身份认证机制，且后端直接连接至企业内部文件搜索系统。攻击者借助提示词注入技术，非法读取企业内部存储的 PDF 文件，其中包含银行账户信息、财务审批流程、费用管理制度等高度敏感的商业秘密，导致严重数据泄露事件。

3.AI 工具部署时因云存储系统配置错误致内部敏感数据泄露

事例简介：某国 AI 驱动软件开发平台因云存储系统配置错误，导致超过 1.29TB 数据和超过 300 万条记录被公开暴露。泄露数据包括：客户姓名、电子邮件、电话号码及实际地址等个人信息，正在进行和已完成的软件开发计划、客户互动记录，员工内部通信（涉及客户项目、运营挑战及商业策略），财务记录（发票和支付详情）等。这些信息可能导致商业秘密泄露，被恶意行为者或竞争对手利用。此次数据泄露被归因于云存储系统部署配置错误，该系统缺乏足够的安全设置，从而允许未经授权的访问。

4.AI 工具配置不当暴露公网，导致敏感资料被境外 IP 非法访问和下载

事例简介：国家安全部披露典型案例：某单位因直接使用开源框架建立联网大模型，导致攻击者未经授权即可自由访问内部网络，从而引发数据泄露和安全风险。案例显示，某单位工作人员在处理内部文件时，违规使用开源 AI 工具，由于电脑系统默认开启公网访问且未设密码，导致敏感资料被境外 IP 非法访问和下载。国安部发布紧急提醒，对于有开源 AI 使用需求的机关单位，建议推进开源大模型私有化部署，将所有数据存储在本地服务器，切断与互联网的直接连接，从源头保障数据安全。同时，建设配套基础设施，组建专业团队开展系统维护与安全监测，及时修补漏洞、抵御攻击。

2.3 AI 工具使用与权限管理环节的泄密风险

2.3.1 员工不当使用 AI 工具引发泄密风险

敏感数据及信息直接输入风险。在服务条款未对数据及信息用途作出限制或使用公有消费级 AI 工具的情形下，员工将包含商业秘密的源代码、核心技术文档、未公开财务数据、客户名单、产品配方等信息及数据输入 AI 工具进行分析或处理，相关商业秘密可能被留存或用于服务优化、模型训练。员工向 AI 工具上传带修订记录、隐藏批注的文档，或截取附带窗口路径、后台标签的界面截图时，AI 工具可能通过图像识别、像素解析捕获隐蔽涉密信息，进而引起商业秘密泄露。

对话交互与碎片化信息组合还原风险。员工通过提示词、上下文补全或示例引导进行交互问答时，AI 工具可凭借其逻辑推理、逆向拆解和关联推演能力，可能将多轮对话中的零散非涉密信息进行整合，反向推导、还原出未直接输入但属于保密范围的信息片段。

“影子 AI” 风险。员工对使用 AI 工具可能引发的商业秘密泄露风险及后果认知不足，私自绕过审批流程使用未经批准的 AI 工具或未经授权的 AI 功能处理涉密业务，往往成为商业秘密泄露的隐蔽通道。

表层脱敏失效风险。员工对涉密信息进行脱敏处理后输入 AI 工具，但人工脱敏过程有可能存在遗漏、不彻底、无效脱敏等问题，AI 工具可依托自身海量知识库及数据关联能力对脱敏信息进行一定程度的还原。如可通过业务规模、合作周期、地域特征反向还原被脱敏的客户主体。

【相关事例】

1.某企业员工将企业涉密信息以提问的方式输入至某 AI 助手，导致半导体涉密数据直传海外

事例简介：2023 年 3 月，某企业允许部分半导体业务部门员工使用某外部通

用型 AI 问答助手，短时间内曝出多起涉密资料外泄事件。经调查，泄密原因均为员工将涉及业务核心的数据或代码直接以提问形式输入该 AI 工具所致。案例一为某企业设备解决方案部门的职员 A 在半导体设备测量资料库下载软件时，发现源代码出现错误，便将有问题部分复制到 AI 工具中寻找解决方案。案例二同样发生在设备解决方案部门，职员 B 将用于识别产品良率的程序代码输入进 AI 工具，要求其优化代码。案例三是该部门的职员 C 为了制作会议记录，将手机上的会议内容转换为文档，之后将文档输入进 AI 工具。前两起案例已分别导致某企业的半导体设备测量资料、产品良率等涉密内容录入到 AI 工具的学习资料库中，内部信息瞬间外泄，且无法收回。某企业方面回应，已加强 AI 工具相关的安全措施，将进一步收紧内部监管和员工培训。此外，某企业还特地发布公告叮嘱员工注意使用 AI 工具的方式，如果再次发生类似事件，内部可能会切断 AI 工具服务。

2.企业员工私用 AI 工具且违规带入办公场景，导致企业泄漏数万条涉密数据

事例简介：2024 年 7 月，某大型娱乐企业员工 A 收到一条私信：“我掌握了你私人生活和工作的敏感信息。”对方不仅复述了他几天前在某工作群里的聊天内容，还陆续抛出了他的信用卡号、社保账号，甚至家中智能摄像头的登录密码。第二天，黑客在网上公开了超过数万条企业内部消息，包括客户隐私信息、员工护照号码、主题公园及流媒体收入数据。事后调查发现，这一切的源头竟是一款“免费 AI 图像生成工具”。2024 年 2 月，员工 A 在自己家用电脑上从某应用程序下载了这款工具，表面上是正常的修图软件，实则内置了恶意程序。黑客借此植入了键盘记录木马，劫持了他存储所有密码的密码管理器。更致命的是，密码管理器没有开启双因素认证，黑客获取主密码后，提取了里面数百个账号口令，直接登录了某企业内部系统，潜伏了五个月后才突然发现。这是典型的“影子 AI”风险——员工未经公司审批，把个人设备上的 AI 工具带进工作环境，却成了黑客入侵企业的完美跳板。

2.3.2 AI 工具账号管理不当引发泄密风险

私人终端登录企业 AI 工具账号。员工使用未经授权的个人终端设备登录企业 AI 工具账号，历史交互记录可能被自动同步至私人设备终端。由于私人设备终端通常缺乏企业级安全防护能力，一旦设备丢失、被盗或转借，其中涉密的历史交互记录存在外泄风险。

AI 工具账号共用风险。员工未经授权与他人共享个人登录凭证，或擅自使用他人账号访问 AI 工具，该账号下的历史对话记录、上传文件及生成内容通常对所有共用者开放可见，增加商业秘密泄露风险。同一账号被多人使用，一旦发生敏感信息输入、下载或对外发送，难以锁定具体人员，泄密事件追责受阻。

闲置账号未注销、权限未回收。企业未及时注销主账号、员工子账号、临时协作账号等，或离职员工、外包人员仍持有 AI 工具登录权限，存在非授权访问历史涉密数据的安全隐患。

第三方应用授权权限未解绑。企业未及时解除 AI 工具与用户 OA、网盘、研发系统、微信等第三方平台的授权绑定，上述接口存在被非授权调用的可能性，历史缓存数据面临被获取的隐患。

【相关事例】

1.员工个人移动端 AI 调用缺乏可验证链路，财务原始数据被“记忆强化”违规传输至境外

事例简介：2025 年 4 月，某跨国金融企业的财务部门引入了最新的 AI 助手（基于大型语言模型）用于日常报表查询。AI 助手通过手机 APP 与企业的 SSO 系统完成单点登录，获得了用户的全部访问权限。企业员工在手机上向 AI 助手询问“上季度的利润率”时，AI 助手在后台自动调用了企业内部 ERP 接口，获取了原始数据并将答案返回给用户。与此同时，AI 助手将查询的原始数据同步至其云端模型进行“记忆强化”，并且在模型训练日志中留下了可追溯的原始数据片段。

该 AI 助手模型所在的云服务位于境外，导致敏感财务数据跨境传输。造成此次泄密事件的主要原因之一在于个人移动端对 AI 调用路径缺少可验证的链路，行为难以审计。

2.某 AI 工具账号共享导致私密数据全面暴露

事例简介：据《华尔街日报》调查，员工在某 AI 工具上共用账号密码已成为普遍现象——员工为节省订阅费用互换登录信息、夫妻共用同一账号讨论家庭事务、小团队为方便共用付费账号等。当个人与工作内容的界限模糊时，包含私人健康信息、机密工作文件或源代码的提示词，对任何拥有密码的人都可见。当多人使用同一登录凭证时，追溯谁上传了什么几乎不可能。生成式 AI 应用会存储持久的聊天历史，任何能访问该账号的人都可以翻阅全部历史记录。

3.AI 工具第三方授权未解绑引发内网数据泄露

事例简介：2026 年 4 月，某海外知名云平台厂商披露重大第三方 AI 账号权限失控安全事件。该企业员工在日常办公中使用第三方 AI 分析工具，并向该 AI 工具授予了其企业账号的完整 OAuth 授权，允许 AI 工具关联、读取员工企业账号资源。后续该第三方 AI 服务商平台被黑客攻陷，攻击者利用企业长期未解绑的 AI 授权凭证，直接劫持、接管该员工的云平台企业账号。攻击者依托失控的企业账号权限，横向渗透进入企业内网系统，批量读取平台环境变量、业务配置、项目密钥等敏感内部数据。本次事件核心成因在于，企业对第三方 AI 工具授权无生命周期管控——员工授予 AI 工具的账号权限长期留存、未定期审计、终止使用后未及时解绑，导致企业合法账号被外部 AI 供应链劫持，账号权限完全失效、失控，引发内部商业数据泄露风险。

2.4 AI 工具更新与退出环节的泄密风险

日志留存管理不当风险。AI 工具平台通常会详细记录 AI 交互内容、文件上传下载行为、账号 IP 及设备信息等操作留痕，其中不可避免包含

商业秘密。企业未对操作日志设置严格访问权限，长期留存的涉密日志易被非法调取、滥用，引发泄密风险。

AI 工具数据残留引发泄密风险。AI 工具停用、更换服务商、系统下线时，未彻底清除云端、本地、备份节点的涉密缓存数据、模型训练残留数据，残留数据长期留存引发后续泄密隐患。

【相关事例】

1.某 AI 大模型数据缓存未清空，导致跨用户隐私泄露

事例简介：2026 年 4 月 20 日，用户张先生让某 AI 大模型翻译英文 PPT，系统未按指令回复，反而返回一份陌生人（钟先生）的完整真实简历，包含姓名、手机号、邮箱、完整工作经历等敏感隐私信息。简历主人证实曾用 AI 大模型润色简历，属于非公开上传内容，两用户操作间隔仅约 6 小时。大模型官方先解释为 AI 幻觉，后改口称是系统“发串”，即把其他用户数据错误分发，未说明具体技术原因。该事件属于典型的“多用户缓存共享但数据隔离未做好”导致的泄露。

3 如何有效防范 AI 工具应用中的商业秘密泄密风险？

在 AI 工具深度嵌入业务场景的当下，新型泄密风险日益增多，传统管理手段已难以全面应对。商业秘密保护是一项系统工程，需从制度、组织、流程到技术全方位布局。本章在梳理传统商业秘密管理策略的基础上，进一步聚焦 AI 工具应用全生命周期的新型泄密风险，引入服务商准入管理、网络安全防护以及多层次技术防护等针对性措施，旨在帮助企业构建更加严密的商业秘密内部管理框架。

AI 工具应用环节	关键制度/措施	具体操作要点	风险管控目标
嵌入 AI 工具应用全生命周期管理	管理制度建设：涉密载体管理、研发合作、设备安全、网络安全、区域管理、人员管理、AI 工具使用规范等	将 AI 工具应用纳入现有保密管理体系；明确禁止将涉密信息上传至公有 AI 工具；建立泄密应急预案，针对 AI 场景细化响应流程等	构建商业秘密管理制度体系，覆盖 AI 工具应用全场景
	管理机构：决策层→管理部门→部门保密员	设置保密部门或专职/兼职保密人员；明确管理层、部门、各人员在 AI 工具应用过程中的保密职责	设立专责机构，明确分层职责
	商业秘密分级分类管理；负面清单管理	密级标识；核心/重要商业秘密禁止输入任何公有消费级 AI 工具，普通商业秘密须脱敏+审批后上传；负面清单动态更新，全员公示	实施密级划分与负面清单管控
AI 工具采购与准入环节	AI 工具服务商合规尽调	优先选择无泄密历史、行业口碑好的 AI 工具服务商	源头把控，防范服务商自身潜在安全风险
	AI 工具白名单管理；官方渠道获取稳定版本	拦截未审批 AI 工具应用；禁止第三方镜像、破解版、停更版本；严禁员工私自下载安装 AI 工具	防范员工私自下载非官方渠道的 AI 工具，引入已知或未知漏洞

AI 工具应用环节	关键制度/措施	具体操作要点	风险管控目标
	第三方插件及技能包准入评估；开源软件准入清单	从官方渠道获取第三方插件、智能体技能包等相关产品，排查窃取、后门、投毒风险；禁用强“传染性”开源协议处理核心业务	防范第三方插件、智能体技能包及开源组件后门、越权访问风险
AI 工具部署与配置环节	本地化/私有云部署；沙箱/虚拟机隔离；云桌面分区	优先采用本地化或私有云部署，确保数据不出域，物理隔离；沙箱/虚拟机隔离部署，沙箱禁止访问核心数据库；AI 操作限定在独立虚拟桌面，与办公桌面隔离	防范公有云部署导致商业秘密泄密，或遭受非法访问，确保运行环境安全可控
	最小权限原则；安全初始化管理	及时修改默认密码、默认端口、数据留存策略等通用配置参数；按需设置高强度专属管理密码、自定义服务端口，关闭非必要冗余服务并收紧开放权限	依据最小权限原则实施初始安全加固，避免因部署安装时沿用初始默认配置、权限开放过大而导致商业秘密泄露
	禁止未隔离执行代码/工具调用	严禁 AI 工具在业务主机、生产数据库环境等核心生产区域直接执行自定义代码、调用第三方工具或加载外部插件	严禁 AI 工具跨接口调用企业涉密信息及数据
	部署网络安全防护设施；实施网络访问控制	部署防火墙、IDS、上网行为管理系统、终端准入系统、堡垒机、零信任安全网关等网络安全防护产品；限定 AI 工具的网络访问边界，将 AI 工具部署于独立网段	强化网络隔离与访问控制，防止外部攻击者可通过外网入侵 AI 工具运行环境，引发商业秘密泄密事件
AI 工具使用与权限管理环节	保密协议+行为准则+红线清单	签订适配岗位职责的保密协议，清晰界定保密义务；发布 AI 工具应用行为准则，明确红线行为；常态化培训	规范员工使用 AI 工具的行为，提高保密意识
	统一账号管理；多因素认证	禁止私人终端登录；远程访问须 VPN+多因素认证实现；离职/调岗员工及时注销 AI 工具账号权限；关闭 AI 工具自动同步、云端	严控账号权限与身份认证，防止账号共用导致操作无法溯源等风险

AI 工具应用环节	关键制度/措施	具体操作要点	风险管控目标
		备份，单次使用后清空缓存	
	部署 DLP 及技术防护手段；统一 API 接口管控	DLP 实时阻断涉密资料上传；设置 CPU/内存上限，防止资源滥用；API 接口加密+限流+参数清洗，定期渗透测试	防止涉密信息通过截图、复制粘贴、API 调用等途径外泄
	数据传输/存储加密；数据脱敏与匿名化；提示词注入防御	存储日志、交互记录加密；脱敏切断碎片信息与完整密级的关联；区分系统指令与外部输入，抵御注入攻击	存储日志及传输数据加密及脱敏处理，防范商业秘密泄密
AI 工具更新与退出环节	操作日志留存；定期日志审计	留存操作人员、时间、内容摘要、流向；审计重点异常导出、非工作时间访问、涉密泄露风险	留存操作日志，定期审计，及时发现异常泄密行为
	账号/权限全面回收；终端“净室”清理；废旧设备物理销毁	及时注销非正常使用账号；清理客户端、缓存、交互记录；涉密设备实行专业粉碎	退出环节闭环管理，实现商业秘密保护全流程管控
监督、评估与闭环改进	风险整改清单；资料归档与分级管理	违规行为生成整改报告，联动调整权限与策略；全流程材料归档并标注密级，差异化防护	形成“监测-阻断-整改-优化”闭环

企业需结合自身业务规模、商业秘密重要程度、可投入成本等实际情况，合理确定管控措施的范围和力度，在安全与效率、投入与产出之间寻找最优平衡。

3.1 商业秘密管理制度设计与基础保障

3.1.1 商业秘密管理制度建设

企业需结合 AI 工具应用场景、业务涉密等级与管理实际，持续完善商业秘密管理制度体系。对于 AI 工具应用过程中产生的新型商业秘密保护需求，及时纳入既有保密管理制度体系。相关制度可包含以下内容：

序号	制度名称	核心定位/ 管理目标	核心管理要求
1	商业秘密保护管理制度	统筹性总纲文件	明确商业秘密保护工作目标、方针、适用范围、策略与原则；将 AI 工具应用纳入保密管理框架，确立"最小必要、全程可控"等保密原则
2	涉密文件资料（物资）管理制度	涉密载体全生命周期管理	规范涉密载体的生成、传递、使用、保存、销毁全流程管理；明确禁止将涉密信息及文件资料上传至公有 AI 工具
3	研发项目及外部合作管理制度	研发/对外合作中信息交互风险管控	增加 AI 辅助研发及对外合作的风险管控措施，明确使用 AI 编写代码、技术方案等时，禁止向 AI 工具输入算法参数、源代码等商业秘密
4	涉密专用设备管理制度	涉密设备全生命周期安全管控	对承载商业秘密的设备终端实施采购、使用、维护、报废全生命周期管控；规范 AI 工具客户端部署安装、缓存清理、权限管控，严防本地缓存、临时文件、会话日志残留引发泄露
5	网络安全管理制度	互联网环境下的信息传输与存储安全	明确涉密信息在互联网环境下传输、存储的安全规范；禁止将涉密信息在公网环境无防护传输至第三方 AI 工具平台
6	涉密区域（场所）管理制度	物理空间信息安全保障	划定涉密区域等级，设定出入权限与管理规范；明确涉密办公区、数据中心等重点区域 AI 工具使用规范
7	涉密人员管理制度	人员全周期保密责任与行为约束	涵盖聘用、培训、考核、离岗等环节，强化保密责任与行为约束；将 AI 工具合规使用、涉密风险防控纳入涉密人员全周期管理
8	人工智能工具使用管理规范	AI 工具应用全流程管理	规范 AI 工具采购、部署、使用、更新迭代、退出全流程；明确禁止使用的 AI 工具类型、使用权限、信息输入审批流程、数据脱敏原则、日常审计要求及违规追责机制
9	商业秘密泄露事件处置管理制度	泄密事件应急响应与处置	建立泄密事件的报告、调查、处置、善后流程，提升应急响应能力；针对 AI 工具引发的泄露场景制定专项应急响应预案

3.1.2 商业秘密管理机构设置与职责

企业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企业，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。明确管理层、相关部门及各岗位人员在 AI 工具应用过程中商业秘密的保护管理职责与分工。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与管理工作，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 AI 工具应用中的商业秘密保护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 AI 工具应用中的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，保障维权工作进行；
- i)其他与商业秘密保护与管理相关的工作。

3.1.3 商业秘密分级分类管理

商业秘密的识别。AI 工具应用前，企业应全面梳理自身商业秘密。具体操作时，可按照“业务-数据-密点”的逻辑逐层映射，将“某项技术方案”或“某套客户数据”等商业秘密，细化为若干个相对独立的技术要点或信息要素的组合，并为每个密点明确对应的载体，如特定代码仓库路径、特定数据表、特定提示词模板、特定训练日志等。技术类商业秘密应在产生、迭代初期及时分解和固定密点，并保留研发过程记录，从而为后续分级管控和维权提供支撑。

商业秘密分级管理。企业可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，将密级划分为核心商业秘密、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进行标识，例如：“★★★+核心商秘”“★★+重要商秘”“★+普通商秘”。划分

密级后，企业可对 AI 工具应用场景中不同密级信息的访问、使用、传输与操作权限实施分级限定。如针对核心工艺、独家配方、核心代码、重大投融资等核心或重要商业秘密，严禁复制、粘贴、上传、输入任何公有消费级 AI 工具，严禁借助 AI 工具编辑、整理、转写、解读涉密及内部敏感内容；普通商业秘密须经脱敏处理并通过上级审批后，方可输入 AI 工具，且审批全流程留痕。

负面清单。制定《AI 工具涉密信息上传负面清单》，动态更新并全员公示。明确界定可输入 AI 工具的信息范围及审批权限，针对公有消费级 AI 工具从严限制，严禁输入核心及重要商业秘密，针对企业级/私有化部署 AI 工具，普通商业秘密经脱敏处理并履行审批手续后可输入使用。

3.2 AI 工具采购与准入环节的风险防控

3.2.1 AI 工具服务商资质审查

AI 工具合规尽调审查。AI 工具应用前，企业应建立 AI 工具准入评估标准与审批流程，并对拟引入的 AI 工具服务商开展合规尽调审查，优先选择无泄密历史、行业口碑好的 AI 工具服务商。

建立 AI 工具服务商安全评估表。核查 AI 工具服务商主体资格、合规资质、数据安全认证资质，确认其具备商业秘密保护能力。

安全能力评估：企业可对 AI 工具服务商进行全面的安全技术评估，评估维度包括但不限于：AI 工具服务商是否支持有效的数据逻辑隔离或物理隔离、数据传输和存储是否采用加密算法、系统是否存在已知安全漏洞，以及 AI 工具服务商对漏洞的发现、响应和修复能力是否符合要求等，以技术检测结果为 AI 工具服务商合规评估提供客观依据。

保密信誉评估：查询 AI 工具服务商过往保密记录、侵权纠纷及泄密

历史情况，避免选择有泄密历史的 AI 工具服务商。

跨境风险评估：检测 AI 工具是否完成数据出境合规、算法与大模型备案，是否满足数据本地化要求，对高风险 AI 工具予以预警标记。

用户协议评估：核查用户协议是否明确约定 AI 工具服务商的数据处理边界、数据留存期限与目的，是否提供不用于训练或服务优化的选项及关闭方式，是否明确数据权属、保密义务、泄密违约责任及数据删除流程。

3.2.2 AI 工具白名单管理

建立 AI 工具白名单管理机制，全面审查 AI 工具是否完成生成式人工智能服务备案（大模型/算法备案）、是否具备网络安全等级保护及数据安全相关认证等。经审查评估合格的 AI 工具，纳入白名单管理，实施准入审批与名单管控。

建立覆盖对话问答、代码开发、图像生成、办公协同等场景的 AI 工具识别库，明确 AI 工具名称、版本、适用场景及使用规则。通过网络出口与终端安全防护联动，拦截未经审批的 AI 工具访问，严禁员工私自下载、安装或使用未经审批的 AI 工具。

已准入的 AI 工具应从 AI 工具官方网站、官方应用商店等渠道获取最新稳定版本进行统一安装部署。严禁使用第三方镜像版本、破解修改版本、历史停更版本及非官方渠道发布的 AI 工具产品，防范恶意代码植入、后门程序及非授权数据收集等安全风险。

3.2.3 第三方供应链准入管理

将 AI 工具所依赖的开源组件、第三方插件、技能包、云储存商等供应链上下游纳入准入管理范畴，建立第三方供应链准入白名单机制。第三

方插件、技能包的提供者与 AI 工具服务方，依照各自与企业的法律关系和合同约定承担责任。

第三方插件与技能包准入管理。AI 工具如需安装第三方插件、智能体技能包（Skills）或拓展程序等，应全面排查是否存在数据非法窃取、权限恶意调用、记忆投毒、代码后门、漏洞植入等安全风险，经安全评估确认无隐患后方可安装使用。从官方渠道获取相关产品，严禁安装或使用任何宣称可“越狱”“突破限制”的产品，审慎授予权限并遵循最小化原则。

使用过程中持续跟踪相关插件及技能包的版本迭代动态、安全漏洞通报及风险预警信息，定期开展安全复核。对存在安全隐患或漏洞无法修复的组件，及时采取停用、卸载、版本升级或替换整改等处置措施。

明确限定插件与技能包的权限范围，禁止读取、同步 AI 交互过程中涉及的信息，关闭自动同步与跨平台传输功能，防止商业秘密通过插件或技能包等渠道跨平台泄露。

建立开源软件准入清单。对 AI 工具中引入的开源组件及依赖链开展前置安全测评，识别后门程序与静默数据回传行为，及时替换风险组件并定期更新安全补丁。明确禁止使用具有强“传染性”的开源协议组件处理企业核心业务，防范商业秘密泄露风险。

3.3 AI 工具部署与环境配置环节的安全加固

3.3.1 AI 工具部署环境安全管控

AI 工具在部署应用前，企业应完成基础安全配置与环境隔离措施，确保运行环境安全可控。

本地化或私有云部署。优先采用本地化或私有云部署模式，确保数据

全生命周期不出域、物理隔离。结合商业模式，对公有云 AI 服务与本地私有化大模型实施分级权限管理，涉及核心、重要商业秘密的场景，禁止接入任何公有云 AI 服务；对普通商业秘密，经脱敏与审批后，可使用通过安全认证、支持数据逻辑或物理隔离、并以合同承诺数据不出域、不用于训练的企业级公有云 AI 服务。

沙箱/虚拟机隔离部署。根据商业秘密等级，制定 AI 工具部署模式的分级选型，实现安全策略与密级精准匹配。处理涉密业务的 AI 工具应统一部署于沙箱或虚拟机隔离环境中，隔离本地临时缓存、交互日志与输出文件，沙箱环境应禁止访问核心数据库、运维终端等敏感资源；沙箱网络出口严格管控，仅放行业务必需接口，阻断非授权外联行为。

云桌面分区管理。为 AI 工具配置独立的虚拟桌面，与企业员工的办公工作桌面进行隔离。AI 工具的所有操作、数据读写均限定在云桌面内，防止 AI 工具越权访问本地数据。

安全初始化管理。针对 AI 工具默认配置中存在的安全隐患，安装后及时修改默认密码、默认端口、数据留存策略等通用配置参数。按需设置高强度专属管理密码、自定义服务端口，关闭非必要冗余服务及开放权限，遵循最小权限原则完成初始安全加固。

禁止未隔离执行代码/工具调用。严禁 AI 工具在业务主机、生产数据库环境等核心生产环境直接执行自定义代码、调用第三方授权工具或加载外部插件。

3.3.2 网络安全防护措施

部署网络安全防护设施。部署防火墙、入侵检测系统（IDS）、上网行为管理系统、终端准入系统、堡垒机、零信任安全网关等网络安全防护

产品，对非可信 IP 地址及未经授权使用的第三方 AI 工具实施访问拦截。

实施网络访问控制。严格限定 AI 工具的网络访问边界，将 AI 工具部署于独立网段，与企业核心业务系统、数据中心、内部办公网络实施物理或逻辑隔离。明确禁止涉密终端直接接入公有云 AI 服务平台，禁止涉密信息在未经审查管控的情况下跨网络流转。

3.4 AI 工具使用及权限管理环节的风险管理

3.4.1 员工 AI 工具使用行为管理

商业秘密保密承诺。企业可根据自身保密管理制度，针对新入职、岗位调整、涉密在岗员工，签订适配岗位职责的专项保密协议。清晰界定员工在 AI 工具应用过程中的保密义务、行为红线及违约追责标准，压实岗位保密责任，强化全员 AI 合规风控意识，从源头防范人为泄密风险。

规范员工信息输入及交互行为。企业应制定并发布员工 AI 工具应用行为准则，明确 AI 工具信息输入与交互的合规要求。同时配套发布员工禁止行为红线清单，明确禁止员工通过公有云 AI 平台以任何形式上传、导入或交互企业核心技术信息、涉密数据、客户隐私、未公开经营资料及其他属于商业秘密范畴的内部信息，确保行为边界清晰可循、合规要求落地可执行。

规范内容生成输出行为。企业可建立 AI 工具生成内容的合规审查机制，员工使用 AI 工具生成的报告、方案、图纸、报表等，需经涉密排查、确认不含商业秘密或敏感信息后，方可内部使用或对外输出。同时，严格禁止员工以转发、截图、分享、外传等任何形式传播含有商业秘密或敏感信息的 AI 生成内容，将违规行为纳入保密考核与责任追究体系。

开展常态化合规培训。常态化组织开展 AI 工具安全合规使用专项培

训，重点讲解私自使用非合规 AI 工具、无意识泄密、违规投喂涉密信息等行为的安全风险与追责处罚标准，普及数据脱敏、分级使用、事前审批等标准化操作规范，全面提升全员 AI 合规使用能力与保密风控意识。

落实日常动态监督管控。对员工 AI 工具应用场景、操作行为、数据交互全过程开展动态监测，识别违规上传涉密信息、私自使用未授权 AI 工具、异常账号操作等风险行为。对排查发现的违规问题即时核查、及时劝阻、限期整改，实现 AI 应用风险早发现、早处置。

3.4.2 身份认证与账号安全管理

企业 AI 工具账号统一管理。明确禁止私人终端设备（包括但不限于私人手机、电脑及平板等）登录企业 AI 工具账号，所有 AI 工具账号须统一通过企业配发并部署安全防护系统的办公终端进行访问，拦截来自非授权终端的登录尝试。

针对远程办公、外部访问 AI 工具需通过 VPN 通道（虚拟专用网络）、多因素认证实现，严格限定访问时间与权限，保障数据传输与访问安全。

细化账号权限管控规则。针对经企业评估获批使用的 AI 工具，实行“一人一号、专属专用”的 AI 工具账号管理制度，严禁员工私自共享登录凭证、转借账号、使用他人账号操作 AI 工具。关闭 AI 工具账号多人共用权限功能，对异地登录、异常设备登录等情况及时预警和处置。

常态化开展 AI 工具账号与使用权限梳理排查，对离职、调岗、离岗员工，及时注销或回收其 AI 工具使用权限，防范终端遗留涉密会话记录。

最小必要权限管控。严格按照岗位配置 AI 工具使用的最小必要权限，所有授权、权限变更全程留痕，从根源杜绝高权限泛滥、违规授权等问题。所有 AI 工具只开放任务所需最小文件夹权限，删除、修改等高风险操作

强制开启人工确认，避免 AI 工具全自动无干预执行危险命令。使用 AI 工具前，关闭自动同步、云端备份、记录公开、智能分享等功能，单次使用结束后，及时清空对话记录、删除上传的所有文件、清理缓存数据，避免在第三方平台留存任何工作信息与敏感内容。

升级多因素强认证机制。对 AI 工具的身份认证体系进行全面升级，摒弃单一密码的弱认证模式，启用“账号密码+人脸核验+设备绑定+动态令牌”等多因素组合认证机制，确保账号操作行为可追溯至具体责任人。

AI 工具账号安全运营。建立账号密码定期强制更新机制，避免弱口令和通用口令。自动识别暴力破解、异地异常登录、非工作时间高频访问等风险行为，一旦触发即自动锁定账号并同步向安全管理员发送预警通知，实现快速响应。

3.4.3 AI 工具运行技术防护措施

部署数据防泄露（DLP）系统。部署 DLP 系统，实时识别涉密提示词输入、涉密文档上传、携带隐藏批注或水印的截图上传等行为并予以阻断。可结合浏览器隔离技术，允许员工正常处理常规任务的同时，在后台自动拦截特定类型数据（如源代码、客户名单、财务数据等）的上传行为，实现“无感知防护”。同时，系统应具备完整的后台日志记录与审计功能，如实留存涉密提示词识别、敏感文档拦截等操作记录，确保商业秘密管理制度及保密防护措施切实执行、有据可查。

支持差异化策略配置，允许普通文本 AI 对话，禁止员工向 AI 工具上传图纸、合同、核心报表、源代码等涉密文档，阻断文件上传通道，避免内部文件被第三方大模型读取存储。

AI 工具运行技术约束。企业可以通过多维度技术限制，约束 AI 工具

运行权限与资源消耗，防范因资源滥用或异常行为引发的失控风险。

a)资源配额限制。针对 AI 运行环境及工具执行环境，如对 CPU、GPU、内存、存储空间等核心计算资源设置资源配额上限或单任务消耗阈值，防止 AI 工具过度占用系统资源或发起资源攻击。

b)任务时长限制。为 AI 工具处理任务配置明确的执行时限，杜绝程序无限循环、长期占用资源等异常情况，保障系统稳定运行。

c)交互长度限制。对 AI 工具单次输入及输出内容的长度施加合理阈值约束，有效规避超长文本交互引发的程序异常、注入攻击等风险。

d)调用频率限制。设置 AI 接口调用频次上限，防范高频滥用、DDoS 攻击（分布式拒绝服务攻击）等恶意行为，保障服务稳定性。

统一 API 接口管控标准。规范 AI 工具 API 接口的调用管控规则，统一配置身份认证、调用频次限流、传输加密、参数清洗、涉密数据过滤等防护措施。严禁通过 API 接口批量外传商业秘密，从接口层封堵无管控的数据流出通道。

定期对 AI 工具 API 接口开展安全漏洞扫描与渗透测试，及时发现并修复接口层安全隐患。对异常调用行为（如高频请求、非授权访问、异常数据包等）实施动态拦截，确保接口层不成为数据泄露的薄弱环节。

办公软件安全管理。对办公使用的软件进行安全评估，确保软件无安全漏洞，及时更新版本并修复已知安全漏洞。对软件使用实施授权管理，防止未经授权的复制和使用。严禁在企业终端设备上私自安装盗版软件或未经安全审查的软件，严防因软件来源不可信而引发系统入侵、数据泄露及合规风险。

3.4.4 数据传输与存储安全管控

提示词注入攻击技术防御。对进入 AI 工具上下文的数据进行标记，严格区分系统指令与外部不可信输入，从技术层面抵御提示词注入攻击，保障 AI 指令执行的安全性与准确性。

数据加密传输与存储。对 AI 工具交互数据的传输链路和存储介质启用高强度加密算法。存储环节对日志缓存、模型交互记录等实施加密保护，确保数据在传输和存储状态下均保持密文形态。

实施数据脱敏与匿名化预处理。对确需输入 AI 工具进行分析的数据及信息，建立深度脱敏处理机制，通过掩码、哈希替换、标识去除、参数隐匿等方式，对项目代号、内部编号、核心参数、客户标识等涉密信息进行改写与模糊化处理，切断碎片化信息与完整商业秘密的关联关系，防范 AI 反向还原涉密内容。

3.5 AI 工具更新退出环节的管理

操作日志留存与归档。系统留存 AI 工具操作日志，包括操作人员账号、终端设备、操作时间、输入输出内容摘要、外网访问流向等信息，支持生成文件流转链路图谱，确保每一次交互行为均可追溯。

明确日志留存期限，采用 WORM（一次写入多次读取）存储介质或区块链存证技术，确保日志在留存期内不可篡改、不可删除。一旦发生泄密事件，确保应能够精准定位至具体操作人，还原 AI 交互过程并固定电子证据，同时作为企业已采取合理保密措施的有效佐证。

操作日志定期审计。定期对 AI 工具使用日志进行安全审计，重点排查高频异常上传、批量数据导出、非工作时段异常访问、涉密信息泄露风险等行为，审计结果应通报相关责任人，并据此优化管控规则。

终端设备“净室”退出。开展办公电脑、办公平板等设备专项清理，

删除所有 AI 工具客户端、登录缓存、涉密交互记录、涉密输出文件等；借助终端安全管理系统进行批量扫描，排查并彻底清除残留的涉密数据，确保终端设备数据清零。

加强私人终端管控，禁止员工通过个人设备或私人账号留存、复用停用 AI 工具所产生的涉密资料；组织员工自查并报备私人终端涉密信息留存情况，定期开展抽查核验。

废旧设备合规处置，对存储过涉密数据的淘汰、报废办公设备，实行物理销毁或专业数据粉碎处理，禁止直接变卖、丢弃，避免泄露风险。

3.6 监督、评估与闭环改进

AI 工具因合同到期、服务变更或业务调整而终止使用时，企业应系统开展内部终端数据清零、权限全面回收及资料归档留存等工作，确保保护措施形成完整闭环，避免“停用即失控”。

全面回收账号与权限。对所有曾接入 AI 工具的账号进行逐一梳理，涵盖主账号、员工子账号、团队共享账号、外包人员账号及第三方系统对接账号，登记账号数量、权限范围和使用责任人。对所有在用、闲置、休眠账号统一注销，关闭所有数据查看、下载、导出、编辑、同步等权限；关闭与 AI 平台的接口对接、数据同步通道，切断后台数据传输链路，避免数据隐形外流。

账号注销、权限回收、接口关闭等操作全程截图、日志留存，记录处置人员、处置时间、处置内容、核验结果，实现全程可追溯。

风险闭环整改。企业在识别员工 AI 工具应用中的违规行为后，应尽快生成整改清单或风险整改报告，详细列明问题类型、影响范围、处置措施及责任归属，作为企业商业秘密保护体系合规运行的重要书面佐证。

同时，联动调整 AI 工具访问权限与保密管理策略，形成“风险监测—实时阻断—证据固定—策略整改”闭环管理，弥补传统纸质制度在动态监督方面的不足。

资料归档与分级管理。系统梳理 AI 工具从准入评估、日常使用到终止退出的全流程资料，将 AI 工具供应商评估材料、保密协议、使用记录、审核记录、终止合作相关文件等统一整理并专项归档。依据商业秘密分级标准，对归档资料分类定级、实施差异化防护，标注对应密级、归档日期和管控责任人，严禁混存、外泄和随意销毁。

4 发生了商业秘密泄露或侵权事件怎么应对与处理？

AI 工具的广泛应用，在显著提升办公效率的同时，也使商业秘密的泄露路径更趋多元化与隐蔽化。本章立足于泄密事件发生后的实操层面，明确侵犯商业秘密的行为，帮助企业精准识别风险性质；其次，提供企业内部应急处置流程，包括阻断传播、固定证据、评估影响等行动；最后，针对泄密事件不同损害程度与维权目标，提供不同维权路径的适用策略。



4.1 侵犯商业秘密行为

企业在应用 AI 工具开展经营活动时，存在商业秘密泄露或被侵犯的风险。对侵犯商业秘密行为的认定，应当严格依据《中华人民共和国反不正当竞争法》（2025 年修订）第十条的规定，结合具体行为的事实与手段进行综合判断。

该条所明确的**侵犯商业秘密行为**包括：

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。

根据《商业秘密保护规定》第十五条的规定，**下列行为一般不属于侵犯商业秘密的行为**：

a)独立发现或者自行研发；

b)对从公开渠道取得的产品进行拆卸、测绘、分析等获得该产品的有关技术信息；

c)商业秘密权利人的前员工利用在工作中积累的通用知识、技能、行业经验，或者通过公开渠道可获取的行业信息开展工作；

d)基于揭露违法犯罪行为、维护国家安全和社会公共利益等需要，依法向国家机关、承担行政职能的法定机构及其工作人员披露商业秘密；

e)其他不属于侵犯商业秘密的行为。

4.2 泄密事件的内部应急处置

企业发现泄密事件，应当第一时间启动内部处置程序，及时控制损害扩大、查明事实真相、追究相关责任、完善制度漏洞。

内部调查。企业应指定内部受理泄密事件报告窗口的负责人或调查小组，重点审查涉 AI 工具使用的操作日志、权限变更记录、外部设备接入记录以及相关人员的即时通讯与邮件往来。对涉事的内部员工、离职人员及合作方人员进行访谈，形成书面调查记录并由被访谈人确认。

应急响应。企业应制定商业秘密泄密紧急处理预案，建立泄密事件紧急应对流程。出现商业秘密泄露时，企业可以采取如下措施：

a)启动紧急处理预案，迅速进行处置，防止信息扩散。

b)证据的收集、固定与保全，证明涉案信息具备商业秘密“秘密性、价值性、保密性”三大法定要件，明确企业合法权属；发现员工有违规上传行为，应立即固化该员工的账号登录时间、设备指纹、所上传文件的哈希值、与该文件相关的 AI 交互输出等电子证据；对容易灭失的 AI 工具留存数据、外网传播内容、云端留存数据、违规操作日志等电子证据，第一时间办理公证保全、区块链存证或第三方证据固化，杜绝证据篡改、删除、失效问题，保障证据法律效力。

c)采取措施，将危害和损失控制在最小限度内。

d)启动对商业秘密泄露的核查、确认和评估，查明原因、责任人。

e)责任追究，对内部人员根据劳动合同、保密协议及企业规章制度，视情节轻重给予纪律处分；涉嫌构成犯罪或严重违约的，依法移交司法机关追究刑事责任或提起民事诉讼索赔。对合作方依据双方签订的合同条款，追究违约方的违约责任，要求其赔偿全部损失，并视情况终止或中止合作关系。

f)开展专项复盘，系统梳理内部管理制度与技术防护措施中存在的漏洞与薄弱环节。针对性地修订保密制度、人工智能工具使用规范及员工手册，将涉人工智能工具的保密管理要求纳入日常合规培训体系。升级技术防护手段，包括但不限于完善数据防泄露系统、实施更精细化的数据分级分类与权限管控等。

4.3 维权途径的选择

对发现的侵犯商业秘密行为，企业可依法主张权利，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。

商业秘密维权案件中，企业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（官方信息发布渠道为 <http://www.cnips.org.cn>），提前筛选具备 AI 技术鉴定能力的机构，掌握其鉴定标准与流程，并在发现疑似侵权线索时，第一时间委托具备知识产权鉴定资质的机构，对涉密 AI 数据、代码、模型输出的同一性进行初步比对，并出具《技术分析报告》。

以下是不同维权途径的路径特点：²

	行政途径	民事途径	刑事途径
立案要求	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	权利人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。	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。
赔偿范围	仅对侵权人/侵权单位行政处罚，不处理权利人经济赔偿问题。一般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。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。
维权周期	取证查处快，维权周期相对较短。	民事诉讼：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。 仲裁：一裁终局，通常比诉讼周期更短、效率更高。	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。
适用场景	行政途径效率高，适合侵权事实清晰、需迅速阻断侵权扩大的案件。	民事诉讼可以主张赔偿和惩罚性赔偿，适合追求经济损失弥补的案件。 仲裁调解程序兼具灵活性与保密性，适合当事人希望快速解决争议的场景。	刑事报案威慑力强，适合侵权情节严重、损失巨大的案件。

²部分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。

4.3.1 行政途径

举报途径。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。向市场监督管理部门提出举报，应当通过全国 12315 平台、12315 热线电话或者市场监督管理部门公布的邮寄地址、受理窗口等渠道进行。深圳市还可通过“深圳 12345 热线”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。

管辖。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。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。经申请授权，深圳市、区两级市场监督管理部门均可独立查办辖区内技术秘密侵权案件。

行政调查措施。市场监督管理部门调查涉嫌侵犯商业秘密行为，可以采取下列措施：（一）进入涉嫌侵犯商业秘密行为的经营场所进行检查；（二）询问被调查的涉嫌侵权人、利害关系人及其他有关单位、个人，要求其说明有关情况或者提供与被调查行为有关的其他资料；（三）查询、复制与涉嫌侵犯商业秘密行为有关的协议、账簿、单据、文件、记录、业务函电和其他资料；（四）查封、扣押与涉嫌侵犯商业秘密行为有关的财物；（五）查询涉嫌侵犯商业秘密行为的经营者的银行账户。

证据准备。权利人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。

权利人的商业信息属于商业秘密的初步证据材料一般包括下列内容：

a)商业信息的形成过程和形成时间；

b)商业信息不为公众所知悉或者不属于《商业秘密保护规定》第六条第二款所列情形；

- c)商业信息的商业价值；
- d)权利人对该商业信息所采取的保密措施；
- e)其他能够证明权利人的商业信息属于商业秘密的证据材料。

下列线索一般可以作为商业秘密涉嫌被侵犯的具体线索：

- a)表明涉嫌侵犯商业秘密的人（以下简称侵权人）有渠道或者机会获取商业秘密的线索；
- b)表明商业秘密的保密措施被涉嫌侵权人以不正当手段破坏的线索；
- c)表明商业秘密已被涉嫌侵权人实际获取的线索；
- d)表明商业秘密已被涉嫌侵权人披露、使用或者有被披露、使用风险的线索；
- e)其他表明商业秘密被涉嫌侵权人侵犯的线索。

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。

4.3.2 民事途径

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。

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³。侵权行为地，包括侵权行为实施地、侵权结果发生地⁴。侵权结果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。

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。

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⁵。

³《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。

⁴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。

⁵《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

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。

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⁶。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。

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。

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。

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。

⁶《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。

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。⁷

4.3.3 刑事途径

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。

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。

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

⁷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。

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。

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一⁸，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⁹。

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。¹⁰

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。

⁸ 《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。

⁹ 《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。

¹⁰ 《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。

附录 1：

AI 工具涉密信息上传负面清单

信息类别	具体描述/示例	风险等级	审批权限	是否绝对禁止	禁止/限制理由
核心、重要商业秘密	未公开的研发配方、核心算法源码、关键生产工艺、战略并购计划、竞标底价、客户核心名单等	高	禁止上传至 AI 工具	是	一旦泄露将造成重大经济损失或市场竞争力丧失
普通商业秘密	常规工艺流程、内部培训材料、一般性合同模板（不含特殊条款）、内部常规管理规定等，具有一般成本投入和普通经济价值，泄露对企业影响程度较小	中	需部门负责人审批，并上传脱敏说明（隐去具体金额、人名、日期等）	否（但须经审批）	有一定商业价值，泄露影响程度较小，经脱敏后可安全用于 AI 辅助分析
日常工作信息	公开会议日程、已发布的产品宣传资料、非涉密的周报摘要等	低	脱敏处理后，员工可上传至 AI 工具	否	安全风险较低，鼓励使用 AI 提升效率

附录 2：

商业秘密保密承诺

（参考文本）

甲方（用人单位）：_____

法定代表人：_____统一社会信用代码：_____

电话：_____传 真：_____

地址：_____

乙方（劳动者、接受方）：_____

居民身份证号码：_____

电话：_____职务：_____

住 址：_____

甲、乙双方根据《中华人民共和国反不正当竞争法》《中华人民共和国劳动合同法》及有关规定，本着平等自愿、协商一致、诚实守信的原则，为保护甲方商业秘密，于____年____月____日签署本保密协议。

第一条 合同目的描述

乙方了解甲方就其产品、研发、制造、营销、管理、客户、计算机（程序）、营运模式等业务及相关技术、服务投入庞大资金及人力物力，享有经济效益及商誉。基于甲方对乙方履行本协议的信赖，乙方知悉参与并接触第三条（保密信息范围的条款）所述各项业务机密资料。乙方若未履行或违反本协议规定，将对第三条（保密信息范围的条款）以及投资、经营、商誉或经济权益产生不利影响，甚至产生直接或间接损害，构成不公平竞争，影响产业公平秩序等，甲方将依据中华人民共和国相关法律、法规等追究其相应法律责任。

第二条 术语定义

本协议所称商业秘密，是指企业在生产经营过程中形成的不为公众所知悉，具有商业价值并经权利人采取相应保密措施的技术信息和经营信息。

本协议所称AI工具，是指甲方使用的或乙方因履行职务接触的生成式人工智能、机器学习、自然语言处理、智能体、自动化决策、数据分析等软件、平台、模型、接口及相关服务，包括本地部署、私有云、公有云及第三方API服务。

第三条 保密信息的范围

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

1、甲方的客户、员工、管理人员及顾问的名单、联系方式及其他相关信息，包括但不限于姓名、联系电话、家庭地址等任何足以识别、联系客户、员工、管理人员及顾问的信息；

2、甲方AI工具应用过程中形成的或与AI工具应用有关的保密信息，包括但不限于：AI提示词、输入内容、输出内容、训练数据、微调数据、知识库、智能体配置、问答记录、使用日志、账号权限、API密钥、模型参数、数据标注规则、AI生成成果及其审核记录等；

3、甲方日常经营管理中的会议决议、会议纪要、谈判与磋商细节等资料；

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

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

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

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

第四条 保密信息的例外

- 1、在披露时或披露前，已为公众所知晓的资料或信息；
- 2、能证明从甲方获得相关信息时乙方已熟知的资料或信息；
- 3、由第三方合法提供给乙方的非保密资料或信息；
- 4、未使用甲方的技术资料，由乙方在日常业务中独立学习或研究获得的知识、信息或资料。

第五条 AI工具应用的保密义务

1、乙方应遵守甲方AI工具使用管理制度、权限分级、审批流程和安全规范，不得越权访问、下载、导出、复制、共享或篡改AI工具账号、数据、模型、知识库、提示词、日志等。

2、未经甲方书面批准，乙方不得将本协议第三条甲方所拥有的商业秘密输入公有云AI工具、外部大模型、插件、浏览器扩展、翻译工具、代码辅助工具或其他第三方服务。

3、乙方应妥善保管AI工具账号、密码、API密钥、访问令牌、证书等凭证，不得出借、共享、泄露或用于非工作目的；发现账号异常、数据泄露、输出敏感信息或被第三方访问的，应立即采取补救措施并报告甲方。

4、乙方使用AI工具生成的内容，应按照甲方要求进行审核、标注、脱敏和合规检查，不得直接对外发布、交付客户或用于决策。

5、乙方应遵守AI工具供应商的服务条款、隐私政策及数据跨境、个人信息保护要求；如发现第三方AI工具可能将输入数据用于训练或披露，

应立即停止使用并报告甲方。

第六条 保密义务的期限

本协议的有效期为本协议签订之日起至双方解除或者终止劳动关系后____年止。

第七条 离职事宜

1、乙方所占有、使用、监督或管理的知识产权有关的资料、机密资料为甲方财产，乙方应于离职时悉数交还甲方并保证不留有任何复制版本。

2、乙方在办理离职手续时，应依甲方要求以书面形式再次确认本协议所述义务，并接受甲方安排的离职面谈，签署相关的承诺书等文件。

3、乙方接受其他用人单位聘用或与他人合伙、合作或合资前，应将签署本协议的相关义务通知新用人单位、合伙人、合作者或合资者。

4、乙方在办理离职手续时，应将甲方AI工具账号、权限、知识库、提示词、输入输出记录、本地缓存、插件、API密钥及其他AI应用相关数据、载体全部交还或按甲方要求删除，不得以任何形式保留、复制、转移、披露或继续使用。

第八条 违约责任

1、乙方违反本协议任何保密义务的规定或不按约定履行乙方的保密义务将构成重大违约行为，乙方须承担违约责任。若乙方的违约行为同时侵犯了甲方的商业秘密等相关权利的，甲方可以选择根据本协议的约定，要求乙方承担相应的违约责任，或根据有关法律、法规的规定要求乙方承担相应的侵权责任。

2、双方约定，在乙方违反本协议约定的保密义务时，若甲方曾向乙方支付保密费的，乙方还应将甲方已经累计支付的保密费全部退还给甲方。乙方承担违约或侵权责任时，除赔偿甲方直接经济损失外，还应包括甲方为维权支付的合理费用。

3、甲方直接经济损失根据甲方销售利润的损失、商业秘密的研究开发费用、实施该项商业秘密的收益（包括合理许可使用费等）、为避免损失进一步扩大而支出的其他补救费用等因素综合计算。

4、乙方违反AI工具应用的保密义务，甲方有权立即暂停或终止其AI工具权限，并按甲方规章制度处理；构成严重违反规章制度的，甲方可依法解除劳动合同。

第九条 合同的解除

双方协商确定，出现下列情形之一的，本协议自行解除或终止：

- 1、保密期限届满；
- 2、甲方宣布解密；
- 3、甲方保密事项已经公开。

第十条 其他

1、本协议自甲乙双方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。

甲 方： （盖章）

法定代表人/授权代表：

日 期：

乙 方： （签字）

日 期：

附录 3：

商业秘密保护相关法律法规（节选）

序号	法律法规名称	核心要点	相关条款
1	《商业秘密保护规定》	什么是商业秘密？	<p>第五条 商业秘密，是指不为公众所知悉、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。</p> <p>与技术有关的结构、原料、配方、材料、样品、样式、工艺、方法、数据、算法、计算机程序、代码等信息，属于第一款所称的技术信息。</p> <p>与经营活动有关的创意、管理、销售、财务、计划、样本、客户信息、数据等信息，属于第一款所称的经营信息。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。</p>
2	《商业秘密保护规定》	哪些情形属于有关商业信息为公众所知悉？	<p>第六条 不为公众所知悉，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。</p> <p>下列情形属于有关商业信息为公众所知悉：</p> <p>（一）该信息在所属领域属于一般常识或者行业惯例；</p> <p>（二）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；</p> <p>（三）该信息已经在公开出版物或者其他媒体上公开披露；</p> <p>（四）该信息已通过公开的报告会、展览等方式公开；</p> <p>（五）所属领域的相关人员从其他公开渠道可以获得该信息。</p> <p>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，符合第一款规定的，属于不为公众所知悉的情形。</p>

序号	法律法规名称	核心要点	相关条款
3	《商业秘密保护规定》	什么是具有商业价值？	<p>第七条 具有商业价值，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。</p> <p>生产经营活动中形成的阶段性成果或者失败的实验数据、技术方案等符合第一款规定的，属于具有商业价值的情形。</p>
4	《商业秘密保护规定》	哪些行为属于权利人采取了相应保密措施？	<p>第九条 本规定所称的权利人采取相应保密措施，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。</p> <p>下列情形属于权利人采取的相应保密措施：</p> <p>（一）签订保密协议或者在合同中约定保密义务；</p> <p>（二）通过建立规章制度、开展培训、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；</p> <p>（三）禁止或者限制进入涉密的厂房、车间、实验室、办公室等生产经营场所或者对其进行区分管理；</p> <p>（四）针对远程办公、跨境协作等场景，采取权限分级、数据脱敏、操作日志留痕等技术保密措施；</p> <p>（五）以标记、分类、隔离、加密、封存、限制能够接触或者获取商业秘密及其载体的人员范围等方式，对商业秘密及其载体进行区分管理；</p> <p>（六）对能够接触、获取商业秘密的计算机设备、网络设备、存储设备等，采取禁止或者限制使用、访问、存储、复制等措施；</p> <p>（七）要求离职员工登记、返还、清除、销毁其接触、获取的商业秘密及其载体，继续承担保密义务；</p> <p>（八）采取其他合理保密措施。</p>

序号	法律法规名称	核心要点	相关条款
5	《中华人民共和国反不正当竞争法》	哪些行为属于侵犯商业秘密的行为？	<p>第十条 经营者不得实施下列侵犯商业秘密的行为：</p> <p>（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；</p> <p>（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；</p> <p>（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；</p> <p>（四）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。</p> <p>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。</p> <p>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。</p> <p>本法所称的商业秘密，是指不为公众所知悉、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。</p>
6	《中华人民共和国反不正当竞争法》	侵犯商业秘密需要承担什么行政责任？	<p>第二十六条 经营者以及其他自然人、法人和非法人组织违反本法第十条规定侵犯商业秘密的，由监督检查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。</p>
7	《中华人民共和国反不正当竞争法》	侵犯商业秘密需要承担什么民事责任？	<p>第二十二条 经营者违反本法规定，给他人造成损害的，应当依法承担民事责任。</p> <p>经营者的合法权益受到不正当竞争行为损害的，可以向人民法院提起诉讼。</p> <p>因不正当竞争行为受到损害的经营者的赔偿数额，按照</p>

序号	法律法规名称	核心要点	相关条款
			<p>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。</p> <p>经营者违反本法第七条、第十条规定，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难以确定的，由人民法院根据侵权行为的情节判决给予权利人五百万元以下的赔偿。</p>
8	《最高人民法院、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》	侵犯商业秘密案件的立案追诉标准	<p>为依法惩治侵犯商业秘密犯罪，加大对知识产权的刑事司法保护力度，维护社会主义市场经济秩序，将《最高人民法院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定（二）》第七十三条侵犯商业秘密刑事案件立案追诉标准修改为：【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：</p> <p>（一）给商业秘密权利人造成损失数额在三十万元以上的；</p> <p>（二）因侵犯商业秘密违法所得数额在三十万元以上的；</p> <p>（三）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；</p> <p>（四）其他给商业秘密权利人造成重大损失的情形。</p>
9	《中华人民共和国刑法》	侵犯商业秘密需要承担什么刑事责任？	<p>第二百一十九条 【侵犯商业秘密罪】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：</p> <p>（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；</p> <p>（二）披露、使用或者允许他人使用以前项手段获取的</p>

序号	法律法规名称	核心要点	相关条款
			<p>权利人的商业秘密的；</p> <p>（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。</p> <p>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。</p> <p>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。</p> <p>第二百一十九之一 【为境外窃取、刺探、收买、非法提供商业秘密罪】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。</p>
10	《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》	侵犯商业秘密刑事案件中，损失数额和违法所得数额如何认定？	<p>第十八条 本解释规定的侵犯商业秘密“损失数额”，按照下列方式予以认定：</p> <p>（一）以不正当手段获取权利人的商业秘密，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；</p> <p>（二）以不正当手段获取权利人的商业秘密后，披露、使用或者允许他人使用的，损失数额可以根据权利人因被侵权造成利润的损失确定，但该损失数额低于商业秘密合理许可使用费的，根据合理许可使用费确定；</p> <p>（三）违反保密义务或者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利润的损失确定；</p> <p>（四）明知商业秘密是不正当手段获取或者是违反保密义务、权利人有关保守商业秘密的要求披露、使用、允许使用，仍获取、披露、使用或者允许他人使用的，损失数额可以根据权利人因被侵权造成利润的损失确定；</p> <p>（五）因侵犯商业秘密行为导致商业秘密已为公众所知</p>

序号	法律法规名称	核心要点	相关条款
			<p>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。商业秘密的商业价值,可以根据该项商业秘密的研究开发成本、实施该项商业秘密的收益等因素综合确定。</p> <p>前款第二项至第四项规定的权利人因被侵权造成利润的损失,可以根据权利人因被侵权造成产品销售量减少的总数乘以权利人每件产品的合理利润确定;产品销售量减少的总数无法确定的,可以根据侵权产品销售量乘以权利人每件产品的合理利润确定。商业秘密系用于服务等其他经营活动的,损失数额可以根据权利人因被侵权而减少的合理利润确定。</p> <p>商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用,应当计入给商业秘密的权利人造成的损失。</p> <p>第十九条 本解释规定的侵犯商业秘密“违法所得数额”,是指因披露、允许他人使用商业秘密而获得的财物或者其他财产性利益的价值,或者因使用商业秘密所获得的利润。该利润可以根据侵权产品销售量乘以每件侵权产品的合理利润确定。</p>