ICS 03 100
CCS A 01

T/AIIA

团 体 标 准

T/AIIA 014—2025

人工智能产业生成合成（深度合成）技术企业商业秘密保护指南

Guidelines for Safeguarding Trade Secrets in Generative AI and Deep Synthesis Algorithms

2025－06－30 发布 2025－07－02 实施

深圳市人工智能产业协会 发 布

目　　次

前言 IV
引言 V
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 总体要求 2
4.1 概述 2
4.2 算法商业秘密保护总体要求 3
4.3 数据商业秘密保护总体要求 3
4.4 代码（开源协议）商业秘密保护总体要求 3
4.5 云服务器商业秘密保护总体要求 3
5 商业秘密信息识别和确定 3
5.1 商业秘密信息的识别 3
5.2 数据准备环节的商业秘密信息确定 4
5.3 模型训练环节的商业秘密信息确定 4
5.4 生成优化环节的商业秘密信息确定 4
5.5 输出控制环节的商业秘密信息确定 4
5.6 应用部署环节的商业秘密信息确定 5
5.7 用户反馈环节的商业秘密信息确定 5
5.8 合规审查环节的商业秘密信息确定 5
6 商业秘密信息管理 5
6.1 分级 5
6.2 存档和保管 6
6.3 流转 6
6.4 备份 6
6.5 复制 6
6.6 发布 6
6.7 加密及解密 6
6.8 销毁 6
6.9 可追溯 6
7 商业秘密管理组织 7
7.1 最高管理者职责 7
7.2 管理部门设置 7
7.3 业务部门责任人 7
7.4 跨部门协作 7
8 商业秘密管理制度 7
8.1 总纲文件 7
8.2 运作机制 7
8.3 企业级管理制度 8
8.4 部门定制制度 8

8.5 管控清单 8
8.6 文件管理 8
9 员工管理 8
9.1 入职管理 8
9.2 保密教育 8
9.3 履职管理 9
9.4 离职管理 9
10 外部人员管理 10
10.1 参观出入管理 10
10.2 保密协议 10
10.3 短期访问管理 10
10.4 长期合作管理 10
10.5 涉密会议管理 10
11 物理区域管理 11
11.1 区域划分 11
11.2 涉密区域管控 11
11.3 数据中心管理 11
11.4 标识管理 11
11.5 出入口安保 11
11.6 网络隔离 11
11.7 外部接待管理 11
12 物品及载体管理 12
12.1 计算机 12
12.2 智能手机 12
12.3 纸质文档 12
12.4 产品 12
12.5 移动存储介质 12
13 信息系统管理 12
13.1 权限管理 12
13.2 账号及口令 13
13.3 信息出口控制 13
13.4 保密措施 13
14 算法模型安全管理 14
14.1 模型访问控制 14
14.2 防逆向保护 14
15 云端安全管理 14
15.1 云服务提供商管理 14
15.2 数据加密 14
15.3 访问隔离 14
15.4 运维审计 14
16 企业数据分类与权属管理 14
16.1 分级保护 14
16.2 流转控制 14
16.3 介质管理 14
16.4 开源数据管理 14

16.5 自研数据管理 15
16.6 合作衍生数据管理 15
17 泄密事件管理 15
17.1 内部管理 15
17.2 证据固定 15
17.3 外部维权 15
18 评估与改进 16
附录A 17
A.1 商业秘密保护范围 17
A.2 竞业限制协议（参考文本） 18
A.3 商业秘密保密协议（参考文本） 22
A.4 不侵犯商业秘密承诺函（参考文本） 27
A.5 商务合作保密协议（参考文本） 28
附录B 31
B.1 商业秘密制度检查表 31
B.2 人工智能产业生成合成（深度合成）算法典型泄密案例库 39
参考文献 42

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由深圳市南山区科技创新局（深圳市南山区创新发展促进中心）提出。

本文件由深圳市人工智能产业协会归口。

本文件起草单位：深圳市南山区科技创新局（深圳市南山区创新发展促进中心）、深圳市南山区工业和信息化局、北京市柳沈（深圳）律师事务所、北京市环球律师事务所、中国质量认证中心、深圳市标准技术研究院、深圳市南山区数字经济产业协会、深圳市宝安区低空无人系统产业协会、深圳市龙岗区未来产业协会、云鲸智能创新（深圳）有限公司、深圳市优必选科技股份有限公司、金蝶软件（中国）有限公司、深圳市东信时代信息技术有限公司、数创弧光（深圳）科技有限公司、沃呈科技（深圳）有限公司、深圳市酷开网络科技股份有限公司、深圳大象安泰科技有限公司、深圳华必选检测认证有限公司。

本文件主要起草人：刘志杰、张景平、申晴、张康康、孟洁、范丛明、朱德财、杨敏娜、江旭晖、易鹏飞、邹海燕、周丹丹、林凯。

引　言

随着经济全球化的不断深化，商业秘密越来越成为企业间、国家间竞争的重要资源。近年来，党和国家高度重视商业秘密保护，陆续出台了一系列商业秘密保护政策。

2024年7月18日，中国共产党第二十届中央委员会第三次全体会议通过《中共中央关于进一步全面深化改革、推进中国式现代化的决定》。其中，在“完善市场经济基础制度”一条中明确提出要“构建商业秘密保护制度”。针对重点领域和重点产业缺乏商业秘密相关保护指引的问题，特别是在人工智能产业的深度合成算法等重点发展方向，制定人工智能产业具体行业的商业秘密保护指南团体标准，是贯彻落实党的二十届三中全会重要部署，进一步探索建立与高水平国际经贸规则相衔接的商业秘密保护体系的必然要求和重要举措。

人工智能产业生成合成（深度合成）技术推动了图像、视频、音频等生成与分析技术的突破性进展，广泛应用于数字娱乐、虚拟现实、广告创意等领域。这类算法的核心价值在于对数据、模型参数、训练方法等核心技术的掌握，其商业秘密保护的需求尤为紧迫，因数据泄露和模型盗用将严重影响企业的市场竞争力。其次，人工智能产业生成合成（深度合成）技术更新迭代快速，导致商业秘密生命周期缩短。传统保密措施可能难以适应持续开发的流程，亟需针对性策略保护核心商业秘密。

在此背景下，本文件旨在为人工智能产业生成合成（深度合成）技术企业提供参考，企业宜按照GB/T22080—2016、GB/T19001—2016和本文件的要求建立、实施、持续改进商业秘密管理体系，结合人工智能产业生成合成（深度合成）技术产业特点，将商业秘密管理贯彻到企业的全部经营活动中，包括但不限于研发、生产、应用、销售、采购、财务、人事、行政、商业合作等。

人工智能产业生成合成（深度合成）技术企业商业秘密保护指南

1 范围

本文件提出了人工智能产业生成合成（深度合成）技术领域企业商业秘密管理的总体要求，商业秘密信息识别和确定，商业秘密信息管理，以及组织、制度、员工、外部人员、物理区域、物品及载体、信息系统、算法模型、云端安全、企业数据分类与权属、泄密事件、评估和改进的管理要求。

本标准适用于人工智能算法方向、人工智能硬件方向和人工智能应用方向的企业或组织，不适用于已通过开源协议公开的算法代码或依法需强制披露的技术内容。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19001—2016 质量管理体系 要求
GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
GB/T 29490—2023 企业知识产权合规管理体系 要求
GB/T 35273—2020 信息安全技术 个人信息安全规范
GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求
GB/T 41867—2022 信息技术 人工智能 术语
GB/T 43782—2024 人工智能 机器学习系统技术要求
GB/T 45225—2025 人工智能 深度学习算法评估
ISO/IEC 27001:2022 信息安全、网络安全和隐私保护-信息安全管理体系-要求
ISO/IEC 22989:2022 信息技术-人工智能-人工智能概念和术语
ISO/IEC 23053:2022 利用机器学习的人工智能框架
ISO 37301:2021 合规管理体系 要求及使用指南
DB4403/T 235—2022 企业商业秘密管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能 artificial intelligence; AI

<学科>人工智能系统（3.2)相关机制和应用的研究和开发。

[来源：GB/T41867-2022，定义3.1.2]

3.2

人工智能系统 artificial intelligence system

针对人类定义的给定目标，产生诸如内容、预测、推荐或决策等输出的一类工程系统。

注1：该工程系统使用人工智能(3.1)相关的多种技术和方法，开发表征数据、知识、过程等的模型，用于执行任务。

注2：人工智能系统具备不同的自动化级别。

[来源：GB/T41867-2022，定义3.1.8]

3.3

生成合成算法 generative and synthetic algorithm

通过机器学习技术自动生成或编辑数字内容的人工智能算法，其输出结果具有非确定性或创造性特征。

3.4

深度合成 deep synthesis

利用人工智能技术实现数字内容生成、修改或增强的技术过程，其输出结果可能产生与真实信息混淆的认知效果。

3.5

商业秘密 trade secrets

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

注1：“不为公众所知悉”、“具有商业价值”和“相应保密措施”的具体内容见《反不正当竞争法》、《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》。

注2：技术信息和经营信息的具体内容可参考附录A.1。

3.6

生成式人工智能商业秘密 generative artificial intelligence trade secrets

不为公众所知悉，具有商业价值，由权利人在技术开发和应用中形成的，采取合理保密措施的源代码、训练数据、优化的模型和独特的算法机制机理等。

3.7

人工智能数据 artificial intelligence data

用于训练、验证和优化人工智能模型的各种数字化信息集合，包括但不限于文本、图像、音频、视频等形式，涵盖真实世界的观测、用户行为记录及专业领域的特定知识等内容。

3.8

涉密物品 secret-related items

含有商业秘密信息的设备和产品。

注：包括计算机、手机、产品、原材料、半成品和样品等。

3.9

涉密载体 secret-related carriers

以文字、数据、符号、图形、图像、视频和音频等方式记录商业秘密信息的介质。

注：包括磁性介质、光盘、U盘、硬盘、服务器等电子存储介质（即涉密存储介质）和纸质材料（即涉密纸质文档）。

3.10

涉密区域 secret-related places

含有商业秘密信息、人员进入后可能接触到商业秘密的物理区域。

3.11

保密义务人 confidentiality obligor

因职务、合同或其他法律关系接触商业秘密的主体。

3.12

合成内容安全隔离 synthetic content security isolation

为防止商业秘密在内容生成过程中泄露而采取的技术管控机制，包括但不限于系统逻辑隔离、加密传输及访问控制。

4 总体要求

4.1 概述

4.1.1 企业宜构建与人工智能产业生成合成（深度合成）产业特点相匹配的商业秘密管理体系，实现商业秘密保护与科技创新效率的协同发展。针对深度合成技术研发、模型参数优化、数据标注等人工智

能行业特有场景及变化，建立动态保护机制。企业的商业秘密管理工作由企业最高管理者牵头，高管负责，专人管理，全员参与。

4.1.2 企业商业秘密信息的管理宜遵循最小授权原则、必须授权原则、审批原则、受控原则、可追溯原则。

4.1.3 企业宜制定商业秘密管理目标，确定保密、效率、成本三者之间的关系。

4.2 算法商业秘密保护总体要求

4.2.1 企业算法商业秘密可能面临数据泄露导致算法暴露等技术性泄露风险，以及内部泄密等管理漏洞风险，需要企业完善相应的商业秘密保护措施。

4.2.2 企业宜建立完善的技术隔离与最小披露制度，通过数据加密、分权访问和硬件级防护，保护算法信息。

4.2.3 企业宜实施分层动态管理，根据技术敏感性和商业价值划分保护层级，匹配差异化措施，并随技术迭代动态调整。

4.3 数据商业秘密保护总体要求

4.3.1 企业数据商业秘密可能面临外部攻击、内部泄露等风险，需要企业针对数据商业秘密构建系统化保护机制。

4.3.2 企业宜对数据收集环节、存储与访问控制环节、模型训练环节、第三方合作管理等多个环节进行数据商业秘密保护。

4.3.3 企业宜建立全流程加密与溯源措施，实现存储传输加密、计算环节加密和部署环节隐匿，并支持泄露溯源。

4.3.4 企业宜建立健全数据分类分级管控制度，并实施差异化加密策略。

4.3.5 企业应严格遵守《网络安全法》《数据安全法》《个人信息保护法》及《网络数据安全管理条例》等数据本地化相关法律法规，在数据跨境传输前进行全面安全评估。

4.4 代码（开源协议）商业秘密保护总体要求

4.4.1 企业代码商业秘密可能面临内部泄露，以及开源合规等风险，需要企业针对代码商业秘密建立多层次防护体系。

4.4.2 企业应明确开源与闭源的边界，建立传染性条款防控机制，以防止核心算法或衍生代码因开源协议限制而被强制公开。

4.4.3 企业宜建立开源代码动态监控机制，监测闭源代码泄露或他人违规复用开源部分未遵守协议的行为。

4.4.4 企业使用开源代码，应遵循相应开源协议条款，如 GPL 协议对于衍生作品商业化闭源的限制、MIT 协议要求修改后的代码或发行包包含原作者的许可信息等，避免产生著作权侵权或合同违约风险。

4.5 云服务器商业秘密保护总体要求

4.5.1 企业云服务器商业秘密可能面临外部攻击、内部权限滥用等风险，需要企业完善相应的云服务商业秘密防护体系。

4.5.2 企业宜在云服务器环境中实施全面加密、隔离与权限管理机制，遵循最小权限原则，确保数据访问控制严格分级，防止内部人员滥用权限或外部攻击获取敏感信息。

4.5.3 企业云服务器数据可采取静态加密、传输加密与运行时保护相结合的策略，确保数据从存储到传输再到计算的全链路加密。

4.5.4 企业宜完善云服务合规机制，全面审查服务协议，明确服务商的数据处理责任与安全义务。

5 商业秘密信息识别和确定

5.1 商业秘密信息的识别

5.1.1 人工智能公司宜围绕生成式人工智能产品的全生命周期，覆盖数据准备、模型训练、生成优化、输出控制、应用部署、用户反馈、合规审查等核心流程，建立差异化商业秘密保护体系。具体技术秘密

和经营秘密的表现形式可参考附录 A.1。

5.1.2　各业务部门经营活动中产生的商业秘密信息宜及时报送商业秘密管理部门登记，商业秘密管理部门宜定期更新商业秘密信息清单。

5.1.3　人工智能产业生成合成（深度合成）产业商业秘密信息范围不限于本文件所示的技术秘密与经营秘密表现形式，企业宜根据技术演进、业务模式创新及司法实践动态，确定各环节的商业秘密信息。

5.2　数据准备环节的商业秘密信息确定

5.2.1　数据采集规则

在数据采集环节，企业宜将用户行为日志的自动化筛选逻辑、高质量数据源的筛选规则以及日志分析机制等作为商业秘密。

5.2.2　清洗标注标准

在数据清洗环节，企业宜将多模态数据的噪声过滤规则、标注质量控制方案、数据增强策略、跨模态对齐技术、流程优化方案、数据脱敏规则等方式作为商业秘密。

5.2.3　合成数据生成

在数据生成环节，企业宜将虚拟数据生成的参数配置、对抗样本设计规则等作为商业秘密。

5.2.4　其他数据准备环节

在其他数据准备环节，企业宜将数据处理技术方案、数据安全防护措施等作为商业秘密。

5.3　模型训练环节的商业秘密信息确定

5.3.1　参数初始化策略

在模型初始化环节，企业宜将权重初始化优化算法、学习率动态调整规则、模型参数等作为商业秘密。

5.3.2　多模态对齐方法

在模型训练环节，企业宜将跨模态特征匹配技术、时序同步机制等作为商业秘密。

5.3.3　训练加速方案

在训练优化环节，企业宜将显存压缩技术、分布式训练的通信优化规则等作为商业秘密。

5.3.4　其他模型训练环节

在其他模型训练环节，企业宜将训练策略优化方案、训练监控与调优方法、模型逆向防护技术等作为商业秘密。

5.4　生成优化环节的商业秘密信息确定

5.4.1　风格迁移参数

在生成优化环节，企业宜将风格控制参数、跨风格融合的对抗训练机制等作为商业秘密。

5.4.2　质量过滤模型

在生成优化环节，企业宜将质量检测算法、实时优化策略等作为商业秘密。

5.4.3　多模态融合技术

在生成优化环节，企业宜将跨媒体关联规则、交互增强方案等作为商业秘密。

5.4.4　其他生成优化技术

在生成优化环节，企业宜将生成控制技术、实时优化系统等作为商业秘密。

5.5　输出控制环节的商业秘密信息确定

5.5.1　动态过滤机制

在输出控制环节，企业宜将敏感内容检测模型、应急响应规则等作为商业秘密。

5.5.2　格式优化方案

在输出控制环节，企业宜将结构化输出技术、多端适配策略等作为商业秘密。

5.5.3　版权标记技术

在输出控制环节，企业宜将隐形水印的嵌入算法、溯源追踪方案等作为商业秘密。

5.5.4　其他输出控制环节

在输出控制环节，企业宜将溯源与审计技术、输出安全与合规控制方法等作为商业秘密。

5.6 应用部署环节的商业秘密信息确定

5.6.1 接口部署方案

在应用部署环节，企业宜将动态令牌生成算法、接口调用频率控制策略（包括分级用户的请求配额分配机制）等作为商业秘密。

5.6.2 本地化部署技术

在应用部署环节，企业宜将边缘计算优化方案、数据缓存策略等作为商业秘密。

5.6.3 客户定制配置

在应用部署环节，企业宜将客户专属知识库的构建规则、功能模块组合策略等作为商业秘密。

5.6.4 其他应用部署环节

在其他应用部署环节，企业宜将安全与访问控制、运维与监控技术等作为商业秘密。

5.7 用户反馈环节的商业秘密信息确定

5.7.1 行为分析模型

在用户反馈环节，企业宜将交互模式识别算法、偏好预测规则等作为商业秘密。

5.7.2 迭代优化策略

在用户反馈环节，企业宜将反馈数据筛选规则、模型增量更新机制等作为商业秘密。

5.7.3 日志脱敏方案

在用户反馈环节，企业宜将用户隐私遮蔽规则、操作日志加密策略等作为商业秘密。

5.7.4 其他用户反馈环节

在其他用户反馈环节，企业宜将用户行为异常预警机制、用户反馈分级分类体系等作为商业秘密。

5.8 合规审查环节的商业秘密信息确定

5.8.1 风险词库管理

在合规审查环节，企业宜将敏感词动态扩展规则、多语种检测机制等作为商业秘密。

5.8.2 审核模型训练

在合规审查环节，企业宜将违规样本标注标准、对抗训练策略等作为商业秘密。

5.8.3 其他合规审查环节

在合规审查环节，企业宜将合规审查流程优化方案、合规风险动态评估模型等作为商业秘密。

6 商业秘密信息管理

6.1 分级

6.1.1 企业宜在经营效率与商业秘密保密需求间寻求动态平衡，通过对商业秘密的科学分级实现精准防护。

6.1.2 企业对商业秘密信息进行评估时，可考虑但不限于以下因素：

a) 商业秘密的性质；
b) 商业秘密的商业价值；
c) 商业秘密的研究开发成本；
d) 实施商业秘密的收益和可得利益；
e) 实施商业秘密可保持竞争优势的时间；
f) 商业秘密的创新程度；
g) 商业秘密信息对企业的重要程度；
h) 竞争对手获取商业秘密后产生的价值；
i) 商业秘密泄露后产生的经济损失；
j) 商业秘密泄露后可能承担的法律责任；
k) 商业秘密信息在企业内部可查阅的范围；
l) 对商业秘密采取保密措施所需的成本。

6.1.3 企业宜根据评估结果将商业秘密信息进行分级管理，商业秘密信息的级别宜在其涉密载体上明确标识。

6.1.4　企业宜分部门建立商业秘密信息清单，内容包括商业秘密信息名称、密级、管理人、载体、查阅范围等。

6.2　存档和保管

6.2.1　各业务部门宜指定专人负责本部门涉密载体的存档和保管。核心商业秘密载体存放建议满足双人双锁，存储区域可配置生物识别门禁系统。
6.2.2　企业宜使用保密柜等具有保密功能的设备来存放涉密载体。
6.2.3　存放涉密载体的区域宜配备监控摄像头、火灾报警等安防设备。

6.3　流转

6.3.1　涉密纸质文档的传递宜采取密封包装、专人专车、EMS 快递等保密措施。核心商业秘密纸质文档流转宜使用防拆封条+GPS 定位包装。
6.3.2　涉密物品等实物的流转，宜采取包装、密封等保密措施。
6.3.3　商业秘密信息在企业内部流转，因工作需要流出到外部需要经过审批。企业宜根据商业秘密信息的级别，设置相应的审批流程、环节和审批部门。外部合作方需签署保密协议。

6.4　备份

6.4.1　企业宜定期对商业秘密信息进行备份，根据商业秘密信息级别的不同分别确定备份保留时间。
6.4.2　企业员工未经审批不能访问备份商业秘密信息，因工作需要临时访问宜由负责人进行审批并保留记录。需记录访问时间、内容、操作行为。

6.5　复制

6.5.1　企业员工未经授权不宜复制或打印商业秘密信息，因工作需要临时复制或打印商业秘密信息宜由责任人进行审批并保留记录。宜禁止使用个人 U 盘拷贝商密文件，仅限使用公司加密 U 盘。
6.5.2　企业员工复制或打印商业秘密信息前宜标明总页数及当前页，打印时必须在打印机旁守候，打印后及时取走不能遗留。打印任务超时未取自动触发碎纸功能。

6.6　发布

6.6.1　对外发布的内容可能包含商业秘密信息的，发布前宜由商业秘密管理部门进行审批。
注：如对外发布论文、网文、产品说明书、用户手册等。
6.6.2　企业宜综合考虑保护策略，合理布局专利保护和商业秘密保护，将两者有机结合更能发挥保护作用，宜用商业秘密保护而不宜公开的内容不宜申请专利。

6.7　加密及解密

6.7.1　商业秘密信息宜通过企业的加密系统进行加密。加密系统宜采取密钥备份、双人控制等安全管理措施。
6.7.2　企业宜指定各部门的责任人或保密员管理各部门的解密权限。员工申请解密的，明确相应的使用人、项目、具体事由、日期。企业宜采取解密申请关联项目编号等方式，以便自动校验申请人权限，以及后续核实项目内容。解密后的信息应及时回收并做相应处理。
注：如解密后文件仅限72小时内使用，超时自动锁定。

6.8　销毁

6.8.1　商业秘密信息载体的销毁过程宜采取监督措施，如视频监控、录像、见证等。
6.8.2　宜根据商业秘密信息载体的不同采取妥善的销毁方式，确保信息不可恢复。纸质文档宜使用碎纸机彻底粉碎；硬盘、U 盘等宜采用消磁的方式彻底销毁存储内容。

6.9　可追溯

6.9.1　所有商业秘密信息的产生、保存、流转、复制、发布、解密、销毁等建议均宜保留记录。记录字段宜包含操作人、时间、操作类型、涉及文件名称等。
6.9.2　记录的留存时间宜根据商业秘密信息的重要性、储存成本决定。

7 商业秘密管理组织

7.1 最高管理者职责

企业最高管理者应具备商业秘密管理意识，保障商业秘密管理资源投入，实现以下关于商业秘密管理的要求：

a) 为建立、开发、实施、评估、维持和改进商业秘密管理配置足够、适当的资源；
b) 确保建立及时有效的商业秘密管理绩效报告制度；
c) 确保战略和运营目标与商业秘密管理相协调；
d) 建立和维护商业秘密泄露事件问责机制，包括纪律处分和后果；
e) 确保商业秘密管理绩效与人员绩效考核挂钩。

7.2 管理部门设置

企业宜设置专门的商业秘密管理部门，或由具备商业秘密管理职能的部门开展商业秘密管理工作。

商业秘密管理部门的组织机构、职责和工作范围可按以下方式确定：

a) 指定专人作为商业秘密管理部门的负责人，负责企业商业秘密管理体系的决策、管理、实施并向企业最高管理者汇报，也可由企业最高管理者直接负责商业秘密管理部门；
b) 配备专职的商业秘密管理人员，或由法务、信息安全等部门人员兼任商业秘密管理工作；
c) 商业秘密管理部门可设立两个以上层级的商业秘密管理组织架构；
   注：如负责决策的商业秘密管理委员会和负责执行决策、统筹管理的商业秘密管理部；
d) 商业秘密管理部门可根据职能设置不同的工作小组，分别负责制度、信息技术、宣传培训、检查评估等工作；
e) 商业秘密管理部门的职责宜包括商业秘密信息、涉密物品、涉密载体、涉密部门、涉密人员、涉密区域等的识别和管理，管理制度的制定、执行、检查、改进，员工的保密宣传、培训、考核，以及泄密事件的内部处理和法律维权等；
f) 商业秘密管理部门可定期组织会议，对商业秘密信息的识别与分级、管理制度的修订、信息技术的实施等重大事项进行决策。

7.3 业务部门责任人

企业宜指定各业务部门的管理者作为各业务部门商业秘密管理的责任人，同时可在重点业务部门配备专职保密员，或由其他员工兼任该部门的商业秘密管理工作，共同负责管理制度在本部门的落地，承担相应的泄密责任。业务部门管理者需与公司签订《保密管理责任书》，明确奖惩条款。

7.4 跨部门协作

企业设立专门商业秘密管理部门的，宜明确商业秘密管理部门和法务部、信息部、审计部等部门的分工，分别负责以下工作：

a) 制定商业秘密管理标准、制度和流程；
b) 组织商业秘密管理宣传、培训、考核；
c) 负责信息技术手段的落地与支持；
d) 处理泄密事件；
e) 监督商业秘密管理工作的执行；
f) 对商业秘密管理体系进行评估与改进。

8 商业秘密管理制度

8.1 总纲文件

企业宜制定商业秘密管理的总体纲领文件，内容可包括商业秘密管理的目标、方针、适用范围、定义、策略、原则等。

8.2 运作机制

企业宜制定商业秘密管理组织的运作机制文件，内容可包括商业秘密管理部门和各业务部门的组织架构、职责与分工、年度工作计划等。

8.3 企业级管理制度

企业宜制定适用于整个企业的商业秘密管理制度，内容可包括：

a) 商业秘密信息的识别与分级；
b) 涉密物品管理；
c) 涉密载体管理；
d) 涉密纸质文档管理；
e) 涉密计算机管理；
f) 涉密网络管理；
g) 涉密区域管理；
h) 涉密人员管理；
i) 泄密事件管理；
j) 奖惩管理。

8.4 部门定制制度

企业宜根据研发、生产、销售、采购、信息技术、财务、行政等业务部门的工作流程和特点，分别制定适用于各个业务部门的商业秘密管理制度。

8.5 管控清单

企业宜编制下列清单以明确商业秘密管理制度的管控对象：

a) 商业秘密信息及分级；
b) 涉密人员及岗位；
c) 涉密计算机；
d) 涉密物品；
e) 涉密信息系统。

8.6 文件管理

商业秘密管理总纲、制度等文件均宜形成企业级文件后在企业内部传达，并持续运行和改进。

注：如制度加密为PDF通过企业OA推送，员工阅读后需电子签名确认，未签署者禁止访问涉密系统。

9 员工管理

9.1 入职管理

9.1.1 涉密人员入职前宜审查其工作背景，审查范围可包括其过往任职的单位、担任的职务、工作内容、是否有涉及知识产权纠纷、是否签署过竞业协议等。

9.1.2 企业宜与涉密人员签订竞业限制协议（见附录 A.2）。

9.1.3 新入职或转岗到涉密岗位的涉密人员应签订与其工作内容相适应的保密协议（见附录 A.3）。高级管理人员、重点项目、商业秘密管理部门员工等重点岗位的涉密人员宜明确其保密范围和接触的商业秘密信息。

9.1.4 涉密人员入职前，宜通过面谈或培训等方式明确告知其保密义务等注意事项，签署《保密义务确认书》，扫描存档至人事系统。

9.1.5 涉密人员曾在存在竞争关系的企业工作过的，入职前可采取以下脱密措施以避免侵害他人的商业秘密：

a) 要求涉密人员提供与原企业的保密协议、竞业限制协议，或其他与保密义务有关的文件；
b) 提醒涉密人员工作中不能使用原企业的商业秘密信息；
c) 签署不侵犯原企业商业秘密的承诺函（见附录A.4）。

9.2 保密教育

9.2.1 企业对员工开展保密教育的内容宜包括以下方面：

a) 商业秘密的重要性；
b) 商业秘密属于企业的职务成果；
c) 侵害企业商业秘密的行为类型；
d) 侵害商业秘密可能承担的法律责任；
e) 企业的商业秘密管理制度；
f) 其他与保密义务、保密范围、保密行为有关的内容。

9.2.2 企业开展保密培训的形式可以是线下、线上集中培训，或录制成视频、音频课程，并保存好培训记录。可通过以下方式对员工开展保密培训：

a) 对新入职的员工开展保密培训；
b) 定期对全体员工开展保密培训；
c) 对重点岗位、重要涉密人员定期开展专项保密培训。

9.2.3 企业可通过以下方式对员工开展保密宣传：

a) 发放员工手册；
b) 定期线上向员工推送宣传案例；
c) 组织答题竞赛；
d) 在办公场所内张贴宣传标语、播放宣传视频；
e) 召开全员保密动员大会。

9.2.4 企业可定期组织员工进行商业秘密保护知识考核，考核结果应归档并整理，用于改进宣传、培训的内容。考核结果可与员工绩效奖挂钩以促进员工增强保密意识。考核题库包含情景判断题,考核结果与奖励挂钩。

9.3 履职管理

9.3.1 员工所在的业务部门宜督促员工熟悉并遵守企业制定的各项商业秘密管理制度，按以下要求以保护员工所在岗位接触到的商业秘密不被泄露：

a) 工作中产生的商业秘密信息应及时上报商业秘密管理部门登记管理；
b) 获取、使用、披露企业的商业秘密信息要有授权或取得临时审批；
c) 获取、使用、披露企业的商业秘密信息要保留相应的记录；
d) 避免非授权人员获取本岗位的商业秘密信息；
e) 不进入非授权区域；
f) 不使用非授权设备、网络、账号。

9.3.2 企业宜建立商业秘密管理奖惩制度。违反企业商业秘密管理规定的处罚结果可形成书面文件，在企业内部通报并存档。鼓励员工举报违反企业商业秘密管理规定的行为，鼓励员工发现企业商业秘密管理体系、措施、技术手段存在的漏洞，对采纳的线索或意见给予奖励。

9.3.3 企业员工参加的工作会议等活动涉及商业秘密的，可采取以下保密措施：

a) 在涉密区域内召开；
b) 使用保密会议室；
c) 参加会议的员工应具备接触所涉商业秘密的权限或经审批；
d) 告知其保密要求或签署保密承诺；
e) 限制使用手机、便携机或拍摄、录音设备，使用防录音装置；
f) 重要涉密纸质文档做好标识，会议后检查并回收。

9.4 离职管理

9.4.1 涉密人员离职前宜与之谈话，告知其保密义务、禁止行为以及违反保密义务的法律责任。

9.4.2 企业应要求离职的涉密人员主动向指定人员移交所有的原始涉密载体且不应删除或篡改，删除其复制的电子数据并签收交接清单。

9.4.3 企业应回收并注销离职员工所有的域名、应用系统、网络系统、门禁系统账号或访问权限，及时通知与离职员工有关的供应商、客户、合作单位等，告知工作交接情况。

9.4.4 涉密人员离职前宜做如下检查：

a) 工作电脑数据是否完整，是否有删除、复制痕迹；
b) 工作电脑上是否有权限之外的文档；
c) 工作系统、软件的账户的访问日志是否有异常；
d) 是否有非工作时间登录、频繁登录、批量下载、删除、修改的异常行为痕迹；
e) 是否有访问外部邮箱的记录；
f) 是否有对外发送商业秘密信息的记录；
g) 检查员工离职前一定期限内的商业秘密信息的查阅和使用情况有无异常。

9.4.5 离职检查过程中如发现离职员工可能侵害企业商业秘密的，宜及时收集并通过公证处对电子证据进行固证,按照企业泄密事件管理规定处理。

9.4.6 企业宜根据需要决定是否对离职员工启动竞业限制，定期掌握涉密岗位离职员工在离职后特别是竞业限制期限内的任职情况。

10 外部人员管理

10.1 参观出入管理

外部人员进入企业应出示证件并履行登记程序，宜佩戴与员工不同颜色的出入卡。访问涉密区域应经审批并进行登记，告知其禁止录音、摄影、摄像、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，并安排专人全程陪同。进入企业参观的，宜设置专门的参观路线以避开涉密区域，参观路线上可能涉及的商业秘密信息应采取隐秘措施。

10.2 保密协议

外部企业需要接触企业商业秘密信息的，应与该企业及相关保密义务人员签订保密协议（具体见参考附录 A.5）或以其他书面形式约定保密义务，内容包括涉密载体、保密范围、保密义务及违约责任等。因诉讼、仲裁等司法活动需要向第三人披露商业秘密信息又无法签订保密协议的，可申请不公开质证或其他保密程序。

10.3 短期访问管理

专家、顾问、律师、会计师等外部人员因工作需要在短期内大量接触企业商业秘密信息的，可要求其使用企业提供的保密计算机并对信息进行加密。需要通过企业内部网络接入涉密计算机或设备的，可通过例如堡垒机采取保密措施。

注：“堡垒机”是指具备监控和记录运维人员操作行为功能的网络安全设备。

10.4 长期合作管理

涉密项目需要长期向供应商或外部研发企业提供商业秘密信息的，或因维修、研发等需要经常进入涉密区域的，可要求外部企业及相关保密义务人员采取以下保密措施：

a) 与参与项目的外部企业员工签订个人保密协议；
b) 增加“第三方连带责任”条款：合作方员工泄密视为合作方违约；
c) 使用企业提供的保密计算机；
d) 使用企业提供的加密系统；
e) 使用企业提供的加密存储介质；
f) 对外部人员使用的便携机等设备进行检查。

10.5 涉密会议管理

与外部人员召开的重要涉密会议，应避免使用远程视频或音频、电话会议。涉密会议宜采取以下保密措施：

a) 在涉密区域内召开；
b) 使用保密会议室；
c) 告知保密要求或签署保密承诺；
d) 采取会议密码、屏幕水印等保密措施。

11 物理区域管理

11.1 区域划分

企业内部的办公区域宜根据商业秘密信息划分为不同的涉密区域，可按涉密区域、办公区域、外部接待区域三级分区。涉密区域可包括核心产品或服务的研发、生产，存储商业秘密信息的数据中心、档案中心等。不同密级的区域之间宜采取物理门、墙、隔断等物理隔离措施。密级高的办公区域宜设置在离企业出入口相对较远的位置。

11.2 涉密区域管控

涉密区域可采取如下保密措施：

a) 使用独立、封闭的办公区域，不宜使用开放式办公或多部门混合办公；
b) 人员进出需具备相应权限且佩戴身份标识卡，非授权人员因工作需要出入需经审批取得临时授权，外部人员进入需有专人全程陪同；
c) 出入口配备安保人员及安防设备；
d) 不应携带手机、便携机、平板、智能手表等具备拍摄、录音、存储功能的设备器材；
e) 不应非授权人员接入涉密网络；
f) 区域内部覆盖实时面部识别、动作识别、异常行为识别的高清摄像头；
g) 内部设置专门的涉密会议室或电话室；
h) 涉密计算机配备防偷窥、防拍照措施。

11.3 数据中心管理

存放商业秘密信息的数据中心、文档中心宜设置在隐蔽的位置，远离非涉密区域且不宜张贴明确标识以防侵入。

11.4 标识管理

涉密区域入口处宜张贴涉密区域级别标识和“禁止携带违禁品”标识，区域内部宜张贴“禁止拍摄”等禁止标识。

11.5 出入口安保

涉密区域的出入口可采取以下安保措施：

a) 使用指纹、人脸识别、瞳孔等技术手段的防尾随门禁，不宜使用刷卡或密码门禁；
b) 配备检测设备以限制携带手机、便携机等违禁品出入；
c) 配备视频监控及报警系统，对非法闯入或携带违禁品进入实时报警；
d) 设置监控中心并配备专职人员实时监控；
e) 设置临时储物柜以存放限制物品。

11.6 网络隔离

企业宜根据业务和保密要求的不同，将内部网络划分为不同的网络区域。涉密区域的涉密网络可采取以下保密措施：

a) 不应接入外网；
b) 与其他内部网络隔离，不能相互连通；
c) 与其他内部网络采取不同的分级管理措施；
d) 禁止使用无线网络、无线热点；
e) 访问涉密区域网络的设备应使用终端准入限制；
f) 不应内部网络设备接入外网；
g) 通过VPN等方式远程接入涉密区域网络应使用终端准入、身份安全等验证措施；
h) 配备独立的网络基础设施。

注：如服务器、防火墙、专线等。

11.7 外部接待管理

企业宜设置专门的外部接待区域用于接待外部人员或用于临时办公、会议，非经审批不应允许外部人员进入内部区域或涉密区域办公。接待区网络与企业内网逻辑隔离，使用独立互联网出口。

12 物品及载体管理

12.1 计算机

12.1.1 涉密计算机宜使用云桌面系统办公以将工作数据存储在内部云服务器上，不宜存储在涉密计算机的本地存储中。
12.1.2 企业宜关闭或禁用涉密计算机的移动存储、光驱、蓝牙、无线网卡等数据传输功能模块，以及摄像头、声卡、话筒等音视频采集设备，未经许可不应使用。摄像头贴防窥贴纸，声卡驱动卸载并设置组策略禁止安装。
12.1.3 涉密计算机硬件的配置、维修、报废均宜经过审批或授权交由指定人员处理，宜使用封条封住主机以禁止员工私自拆机维修、更换、增加硬件配件。维修前签署《硬件操作保密协议》，全程视频监控。
12.1.4 计算机未经批准不宜安装非授权软件。
12.1.5 计算机的网络接入、网络配置宜按规定设置，不宜接入非授权网络。
12.1.6 涉密便携机宜设置身份验证、硬盘口令，封闭摄像头和麦克风功能，存放时使用带锁的保密柜。不宜在涉密区域使用便携机办公。

12.2 智能手机

12.2.1 涉密区域不宜使用个人智能手机。如携带个人智能手机进入涉密区域建议关闭或禁用摄像头、麦克风，不宜在涉密区域内拍摄、录音、设置热点。
12.2.2 个人智能手机不宜接入存有商业秘密信息的软件及信息系统，避免在个人手机内存储商业秘密信息。企业应用容器化，禁止数据导出至个人空间。
12.2.3 个人智能手机不宜接入企业涉密网络。

12.3 纸质文档

12.3.1 涉密纸质文档宜存放在涉密区域内，打印、复印、扫描、查阅、借用等使用涉密纸质文档宜由专人专管并登记。
注：如借阅记录通过二维码扫码登记，自动关联OA系统流程。
12.3.2 企业宜配备打印管控系统管理纸质文档的打印、复印、扫描，并保留记录及备份。打印、复印、传真涉密纸质文档时宜具备授权并在机器旁守候及时取走文档。扫描纸质文档不宜使用公共盘存储。
12.3.3 废弃的纸质文档宜通过碎纸机粉碎，不应随意丢弃。

12.4 产品

12.4.1 涉密项目的半成品、样品宜由专人管理，放置在保密柜或专门的存储室保管，出入口配备摄像头监控。携带外出时宜采取包装等保密措施。
12.4.2 涉密项目的不良品宜交由专人处理或报废，不宜随意丢弃。
12.4.3 涉密产品、半成品、原料等的标签宜替换为企业内部的编码统一管理。

12.5 移动存储介质

12.5.1 未经审批不宜使用移动存储设备存储商业秘密信息。涉密移动存储介质不宜连接非涉密或未采取保密措施的计算机及电子设备。
12.5.2 涉密移动存储介质宜由专人专管，且使用身份识别、内容加密、设备绑定等保密措施。
注：如部署USB端口管控系统，仅识别授权加密U盘。涉密U盘硬件加密，输错密码10次自动擦除数据。

13 信息系统管理

13.1 权限管理

13.1.1 商业秘密管理部门宜统一管理对涉密信息系统的授权及审批。

注：如核心系统权限审批需双人双岗确认。

13.1.2 权限到期、人员变更或离职、项目变更等情况宜及时变更、回收相应的信息系统权限。

注：如集成HR系统，员工调岗/离职时自动触发权限回收,项目结束时系统自动禁用相关访问组。

13.1.3 信息系统的权限管理宜保留记录日志，用于定期检查各信息系统用户的访问权限、特别授权等权限管理是否存在漏洞。

13.1.4 信息系统的管理员权限宜在不同人员之间进行分配，避免由超级管理员管理整个系统或若干个系统的情况。

13.2 账号及口令

13.2.1 业务部门设置公用账号、匿名账号等特殊账号宜经过商业秘密管理部门审批。

注：如公用账号申请需说明使用场景,有效期≤7天,超出应向主管部门说明情况。

13.2.2 外部人员的账号宜与内部员工账号有明显的区别。

13.2.3 账号宜同时包括特殊符号、大写英文字母、小写英文字母、数字四种不同字符。

13.2.4 信息系统账号的初始口令宜为随机产生的口令，不能相同或有规律，且规定修改口令设置的位数、更换周期的最低标准。

13.2.5 信息系统的口令宜通过系统设置强制用户定期更换。

13.3 信息出口控制

13.3.1 未经审批不宜允许任何商业秘密信息外部出口存在。所有经审批的信息出口宜有以下“四统一”：

a) 统一登记；
b) 统一管理；
c) 统一备份；
d) 统一监控。

13.3.2 企业的办公网络不宜允许访问非企业邮箱的外部邮箱，宜将常见的外部邮箱、地址包括网址设为禁止访问名单。因工作需要登录外部邮箱的宜经过审批并备案邮箱账号和密码。

13.3.3 企业宜建立代理服务器访问备份系统，代理服务器访问日志备份 6 个月以上。宜设置访问外网时允许上传的字节数，从而限制通过代理服务器对外发送商业秘密信息。

13.3.4 企业宜禁止员工使用网盘，将常见的网盘网址设为禁止访问名单。确因工作需要登录网盘的宜经过审批，并向企业备案网盘账号和密码。

13.3.5 企业涉密计算机使用的即时通讯软件宜避免和其他外部通讯软件交互商业秘密信息，宜具备以下保密功能：

a) 具备对用户登录进行网络、设备控制的功能，保证其在安全环境下运行；
b) 具备检查聊天内容关键字的后台管控功能；
c) 在移动终端应具备禁止复制、转发、下载和全场景添加水印的管控功能。

13.3.6 企业存储商业秘密信息的云服务器或信息系统宜关闭信息外部出口，未经审批不宜允许在服务器上复制、修改商业秘密信息。操作日志同步至区块链存证平台，确保不可篡改。

13.4 保密措施

13.4.1 涉密计算机的操作系统、办公软件、信息系统等宜设置登录账号，密码宜定期更换，不宜共用账号。

13.4.2 企业宜对操作系统设置屏幕保护恢复密码、屏幕水印、复制粘贴限制等保密措施。

13.4.3 涉密计算机的办公软件宜由企业统一安装并管理，未经授权不宜私自安装软件。个人邮箱、网盘、即时通讯工具等具备通过网络对外发送文件的软件均宜禁止。

13.4.4 企业宜使用具备关键字过滤、外发邮件审批、邮件审计等保密功能的企业邮箱。

13.4.5 在涉密网络内部使用的即时通讯软件不宜与其他网络，或连接到互联网的通讯软件连接。

13.4.6 加密软件宜定期检查，确保加密软件对所有类型文件在所有场景都能够进行加密。批量解密等特殊解密的授权权限宜经过审批统一管理。

13.4.7 企业宜使用专用的信息系统存储商业秘密信息，信息系统宜具备权限管理、日志、审计等保密功能。

13.4.8 涉密计算机宜安装专门的行为管控软件，可记录商业秘密信息数据的复制、流转、删除等操作

并保存备份。

14 算法模型安全管理

14.1 模型访问控制

14.1.1 核心算法参数的访问权限宜经商业秘密管理部门审批，实施动态密钥管理。
14.1.2 开源框架的节点通信可启用双重加密机制，包含传输层加密与应用层加密。

14.2 防逆向保护

14.2.1 核心算法宜采用代码混淆与硬件绑定技术，确保算法无法脱离特定控制器运行。
14.2.2 模型部署包可嵌入数字水印，包含企业标识符。

15 云端安全管理

15.1 云服务提供商管理

15.1.1 宜选择具有权威安全认证、符合相关行业安全标准的云服务提供商，并与云服务提供商签订详细的数据处理协议，明确其在商业秘密保护方面的责任、义务和违约条款，包括数据存储地点、访问权限、加密方式、数据删除策略等。

15.2 数据加密

15.2.1 宜对存储在云端的静态数据和从用户端到云端、以及在云服务内部传输过程中的数据加密。宜建立安全的密钥管理系统，对加密密钥进行严格管理、轮换和保护，避免密钥泄露导致数据泄露。

15.3 访问隔离

15.3.1 研发测试环境宜与生产环境物理隔离，使用不同的服务器和网络设备，禁止共用存储空间，测试数据宜经脱敏处理。
15.3.2 云端 API 调用宜绑定设备指纹，包含控制器序列号与安全芯片 ID。

15.4 运维审计

15.4.1 云端操作日志留存周期宜覆盖项目保密期，关键操作需二次审批。
15.4.2 宜定期执行渗透测试，重点检测算法泄露路径。
注：如发现的高风险漏洞需在3天内修复，并重新测试确认问题已解决。

16 企业数据分类与权属管理

16.1 分级保护

16.1.1 企业宜按照产品智能化等级设定数据保护强度。

16.2 流转控制

16.2.1 企业宜使用专用数据总线传输研发数据，总线协议宜包含报文级加密、终端设备双向认证。

16.3 介质管理

16.3.1 烧录调试工具宜具备防提取功能，擦除固件后自动销毁临时密钥。

16.4 开源数据管理

16.4.1 管理规则

企业应严格遵循开源协议的数据使用限制。

16.4.2 技术实现

企业宜建立代码仓库自动标识系统，通过物理隔离存储开源数据与自研数据。

16.5 自研数据管理

16.5.1 管理规则

企业宜通过贡献者协议（CLA）明确数据所有权，将核心训练数据、用户行为日志纳入企业资产目录。

16.5.2 技术实现

企业宜通过部署数据血缘追踪工具，实现数据全生命周期权属标记。

16.6 合作衍生数据管理

16.6.1 管理规则

企业在合作协议中宜明确联合开发数据的访问权限，例如限制合作伙伴在沙箱环境中访问敏感数据。

16.6.2 技术实现

企业可搭建动态数据沙盒系统，设置基于角色、IP、操作类型的细粒度访问控制。

17 泄密事件管理

17.1 内部管理

17.1.1 企业宜指定内部受理泄密事件报告窗口的负责人，并公开电话、邮箱等联系方式。

17.1.2 企业宜设定泄密事件等级及相应的判定标准，并根据泄密事件等级制定泄密事件处理流程和应对预案，包括但不限于以下内容：

a) 采取保护措施防止信息进一步扩散或损失扩大；
b) 调查原因、涉事人员、责任人等；
c) 收集并固定证据；
d) 启动内部处罚或外部维权；
e) 形成报告和改进方案。

17.2 证据固定

17.2.1 可向专业的商业秘密保护服务机构寻求取证、鉴定、评估等指引和协助。商业秘密信息的非公知性、同一性、损失数额的确定可向有资质的专业机构申请协助鉴定或评估。

17.2.2 发现商业秘密可能被泄露或侵权时，宜收集并固定如下证据：

a) 企业是商业秘密的权利人；
b) 商业秘密信息的具体内容和载体；
c) 商业秘密信息不为一般公众普遍知悉；
d) 商业秘密信息不为一般公众容易获得；
e) 企业对商业秘密信息采取的保密措施；
f) 商业秘密信息具有商业价值；
g) 泄密人员的身份、工作信息；
h) 泄密人员接触到了商业秘密信息；
i) 被控侵权信息与商业秘密信息实质性相似；
j) 泄密人员以不正当手段获取、披露、使用商业秘密信息等反不正当竞争法规定的侵权行为；
k) 因泄密产生的损失或侵权人的获利、许可使用费，以及因维权产生的律师费、鉴定费、评估费等；
l) 产生商业秘密信息的开发费用等成本。

17.2.3 电子数据类证据可向公证处等机构申请公证或证据固化。实物和文档宜拍照存档并标注提取时间、地点及保管人。

17.3 外部维权

17.3.1 可向侵权人所在地等有管辖权的商业秘密行政管理部门举报，要求查处商业秘密侵权行为的证据，责令侵权人停止侵权并处以罚款。

17.3.2 符合刑事案件立案条件的可向犯罪行为发生地的公安机关控告，要求追究侵权人的刑事责任。
17.3.3 违反竞业限制协议等属于劳动仲裁受案范围的，应先向企业所在地等有管辖权的劳动仲裁委员会申请劳动仲裁。
17.3.4 第三方企业违反协议约定的保密义务且约定商事仲裁管辖条款的，应向约定的仲裁委员会申请仲裁。
17.3.5 不属于劳动仲裁且没有商事仲裁约定的，可向侵权行为发生地或侵权人所在地等有管辖权的人民法院起诉，或申请诉前禁令。
17.3.6 如泄露的商业秘密信息涉及国家秘密的，应立即向当地国家安全机关、保密行政管理部门或公安机关报告。

18 评估与改进

18.1 企业宜配备专门的人员负责商业秘密管理的检查，也可由各业务部门保密员负责各部门的检查工作。定期检查保密措施是否到位。
注：如每月抽查文件柜是否上锁、电脑是否加密。
18.2 企业宜采取以下措施并保留记录或原始文件用于检查和评估：
a) 重要涉密区域的出入口和内部应安装监控系统实时监控；
b) 涉密网络的出、入口应实时监控；
c) 涉密计算机的操作；
d) 存储商业秘密信息的信息系统；
e) 对外发送商业秘密信息的软件。
注：如电子邮箱、即时通讯软件。
18.3 宜定期对企业的以下商业秘密管理情况进行评估并形成书面报告提交商业秘密管理部门：
a) 商业秘密管理部门人员的履职；
b) 商业秘密管理制度的适宜性；
c) 商业秘密信息的定密、分级、流转；
d) 涉密纸质文档、物品、计算机的管理；
e) 涉密区域的管理；
f) 操作系统、办公软件、信息系统的账号、权限；
g) 涉密人员的管理；
h) 其他商业秘密管理制度规定的内容。
18.4 针对定期评估报告发现的管理漏洞制定改进方案、实施计划并执行落地，明确责任人、完成时间和验收标准。

附 录 A
（资料性）
商业秘密保密范围及参考文本

A.1 商业秘密保护范围

商业秘密的技术信息保护范围的参考内容见表 A.1.1。

表 A.1.1 商业秘密的技术信息保护范围

项目	表现形式
算法和模型	源代码、神经网络架构、深度学习框架、数据预处理步骤、特征选择等。
数据集和训练资源	训练 AI 模型的专有数据集、数据增强技术、数据隐私保护措施等。
系统架构和设计	硬件和软件的集成方案、定制化部署策略、高性能计算集群的优化技术等。
软件和代码	自主开发的软件工具、库和 API 接口的详细信息、特定的编程代码片段等
研发记录和文档	实验记录、研究论文、技术报告、项目进度文档等。
技术指标和性能参数	AI 系统的准确率、响应时间和资源消耗指标、测试报告等
安全和隐私保护机制	数据加密算法、网络安全防护措施、隐私保护策略等。
测试和验证流程	质量控制和性能测试的方法、故障排除和问题解决的内部指南等。
其他	企业认为有必要采取保密措施的其他技术信息

商业秘密的经营信息保护范围的参考内容见表 A.1.2。

表 A.1.2 商业秘密的经营信息保护范围

项目	表现形式
公司基础信息	公司架构、规章制度、内部通知、决议文件、会议纪要等
决策信息	战略决策、研发策略、投资计划、股权激励方案、专利规划布局等
产品和服务	未发布的产品特性、功能和用户界面设计、定制化服务的客户解决方案等
销售信息	客户名单、供应商名单、销售记录、销售协议、投标书等
财务信息	财务报表、融资报表、预决算报告、各类统计报表、审计报告等
人力资源信息	员工名册、通讯录、工资表、社保公积金清单等
信息技术信息	网络拓扑图、信息安全风险报告、运维日志等
其他	企业认为有必要采取保密措施的其他经营信息

A.2 竞业限制协议（参考文本）

甲　方（用人单位、披露方）：_____

法定代表人：_____　统一社会信用代码：_____

电　话：_____　传　真：_____

地　址：_____

乙　方（劳动者、接受方）：_____

居民身份证号：_____

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》《中华人民共和国公司法》《中华人民共和国劳动合同法》及国家、地方有关规定，双方本着平等自愿、协商一致、诚实守信的原则，就竞业限制事宜，于____年__月__日（以下简称“生效日”）在中华人民共和国_____（具体签署地址）签署本协议以共同执行：

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物力，享有经济效益及商誉；乙方若未履行或违反本协议规定，将对甲方投资、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 竞业限制义务

乙方承诺在竞业限制期间：

1、未经甲方同意，乙方在甲方任职期间不得自营或者为他人经营与甲方同类的营业。不论因何种原因从甲方离职，乙方在劳动关系解除或终止后___年（不超过二年）内，不得到_____（具体竞业限制区域）内与甲方生产或者经营同类产品、从事同类业务的有竞争关系的其他用人单位，或者自己开业生产或者经营同类产品、从事同类业务。

2、乙方为证明在竞业限制期限内已履行了竞业限制义务，自乙方在劳动关系解除或终止后____月内，应及时向甲方提交下列证明材料，以证明自己是否履行了竞业限制协议约定的义务：

（1）从甲方离职后，与新的单位签订的劳动合同，或者能够证明与新的单位存在劳动关系的其他证据；

（2）新的单位为该乙方缴纳社会保险的证明；

（3）或当乙方为自由职业或无业状态，无法提供上述（1）、（2）项证明时，可由其所在街道办事处、居委会（村委会）或其它公证机构出具的关于乙方的从业情况的证明。

3、不得利用其甲方股东等身份以任何不正当手段获取利益，不得利用在甲方的地位和职权为自己

谋取私利。

4、不得直接或间接拥有、管理、经营、控制，或参与拥有、管理、经营或控制或其他任何形式（包括但不限于在某一实体中持有权益、对其进行投资、拥有其管理责任，或收购其股票或股权，或与该实体订立许可协议或其他合同安排，但通过证券交易所买卖上市公司不超过发行在外的上市公司股票 3%的股票的行为除外)从而在竞争性区域内从事与任何在种类和性质上与甲方经营业务相类似或相竞争的业务。

5、不得在竞争性单位或与甲方有直接经济往来的公司、企业、其他经济组织和社会团体内接受或取得任何职务（包括不限于合伙人、董事、监事、股东、经理、职员、代理人、顾问等），或向该类竞争性单位提供任何咨询服务（无论是否有偿）或其他协助。

6、不得利用股东等身份做出任何不利于甲方的交易或安排；不以任何方式从事可能对甲方经营、发展产生不利影响的业务及活动，包括但不限于：利用现有社会及客户资源阻碍或限制甲方的独立发展；对外散布不利于甲方的消息或信息；利用知悉或获取的甲方信息直接或间接实施或参与任何可能损害甲方权益的行为。

7、不得拉拢、引诱或鼓动甲方的雇员离职，且不得自行或协助包括但不限于在生产、经营或销售等领域与甲方经营业务相同及或相似之经济实体招聘从甲方离职之人员。

8、不得在包括但不限于生产、经营及或销售等领域与甲方之包括但不限于原料供应商、产品销售商等各种业务伙伴进行与甲方存在竞争之活动。

9、不得自行或协助他人使用自己掌握之甲方计划使用、或正在使用之一切公开及或未公开之技术成果、商业秘密，不论其是否获得利益。

第三条 竞业限制补偿

1、在乙方竞业限制期间，即与乙方劳动关系解除或终止后____年内，甲方每月向乙方按其离职前 12 个月平均工资（包括年终奖等一切劳动报酬）的____%的标准支付津贴作为补偿。

2、支付方式为：补偿费从____年___月___日开始，按月支付，由甲方于每月的___日通过乙方的银行账户支付。乙方银行账户如下：

开户名称：_____

银行账号：_____

开 户 行：_____

3、如乙方拒绝领取，甲方可以将补偿费向有关机关提存，由此所发生的费用由乙方承担。

第四条 违约责任

1、甲方无正当理由不履行本协议第三条所列各项义务，拒绝支付乙方的竞业限制补偿费（延迟支付约定的补偿费支付期限一个月以上，即可视为拒绝支付）的，甲方除如数向乙方支付约定的竞业限制补偿费外，还应当向乙方一次性支付竞业限制补偿总额_____%的违约金。

2、乙方不履行本协议第二条规定的义务，应当向甲方一次性支付竞业限制补偿总额_____%的违约

金，同时乙方因违约行为所获得的收益应归甲方所有，甲方有权对乙方给予处分。如违约金不足以补偿甲方损失，甲方还有权向乙方主张由此遭受的经济损失。

3、前项所述损失赔偿按照如下方式计算：

（1）损失赔偿额为甲方因乙方的违约行为所受的实际经济损失，计算方法是：因乙方的违约行为导致甲方的产品销售数量下降，其销售数量减少的总数乘以单位产品的利润所得之积；

（2）如果甲方的损失依照第（1）项所述的计算方法难以计算的，损失赔偿额为乙方及相关第三方因违约行为所获得的全部利润，计算方法是：乙方及相关第三方从与违约行为直接关联的每单位产品获得的利润乘以在市场上销售的总数所得之积；

（3）甲方因调查乙方的违约行为而支付的合理费用，包括但不限于律师费、调查费、评估费等，应当包含在损失赔偿额之内。

4、如乙方不能按第二条第 2 项要求提交约定证明材料，则应该视为乙方未履行竞业限制协议约定的义务，甲方有权按本竞业限制协议参考上述条款追究乙方的违约责任。

第五条 合同的权利义务终止

双方约定，出现下列情况之一的，本协议自行终止：

1、乙方所掌握的甲方重要商业秘密已经公开，而且由于该公开导致乙方对甲方的竞争优势已无重要影响。

2、甲方无正当理由不履行本协议第三条的义务，拒绝向乙方支付竞业限制补偿费的。

3、甲方因破产、解散等事由终止法人主体资格，且没有承受其权利义务的合法主体。本协议权利义务的终止不影响甲乙双方在本协议签订之前或之后签订的商业秘密保密协议的效力。

4、竞业限制期限届满。

第六条 纠纷解决程序与管辖

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

（1）向本合同签订地人民法院提请诉讼；

（2）向_____仲裁委员会申请仲裁。

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

第七条 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。

（以下无正文）

甲　方：_____（盖章）　　乙　方：_____

法定代表人/授权代表:_____

日　期：_____　　日　期：_____

A.3 商业秘密保密协议（参考文本）

甲　方（用人单位、披露方）：_____

法定代表人：_____　统一社会信用代码：_____

电　话：_____　传　真：_____

地　址：_____

乙　方（劳动者、接受方）：_____

居民身份证号码:_____

电　话：_____　职　务：_____

住　址：_____

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》及国家、地方有关规定，双方本着平等自愿、协商一致、诚实守信的原则，为保护甲方商业秘密，于_____年___月___日（以下简称“生效日”）在中华人民共和国_____（具体签署地址）签署本保密协议以共同执行：

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；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系基于甲方对乙方履行本协议之信赖。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。

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（移动和固定电话）、电子邮件地址、即时通讯方式或社交网络地址（QQ、MSN、Skype、微信、易信、来往、Line、微博、空间等）、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）与甲方经营活动有关的合同文本及法律文书；

（3）甲方经营活动中涉及的关键价格信息；

（4）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；

（5）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）；

（6）与甲方资产、财务有关的信息（如存货、现金等资产的存放地、保险箱密码、数量、价值等，以及财务报表、账簿、凭证等）；

（7）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）；

（8）甲方的知识产权、专有技术等信息（如产品设计、产品图纸、生产制造工艺及技术、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）；

（9）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，已为公众所知晓的信息或资料；

2、能证明从甲方获得相关信息时乙方已经熟知的资料或信息；

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 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。其中涉及国家机密的，依照《中华人民共和国保守国家秘密法》及相关法律法规的规定执行。

第六条 保密义务的效力

乙方确认，在与甲方的劳动关系存续期间，需在任何地域内遵守本协议约定之保密义务。乙方不得以该地域不能够或者不具备形成甲方的实际竞争关系为理由，要求甲方排除本协议约定之保密义务。

第七条 积极保密义务

1、如乙方须对外使用甲方所披露的信息时，不确定该信息是否为保密信息，需向甲方书面征询，由甲方给予书面答复。

2、乙方应自甲方按要求向其提供保密信息之日起，对相关信息予以保密，不得向任何第三方披露上述信息。

3、为使乙方更好地履行本协议约定之保密义务，甲方应该对乙方进行保密教育及培训。

第八条 消极保密义务

1、乙方于任职期间或离职后所知悉、接触、持有、使用之机密资料及密码，系甲方或其客户赖以经营之重要资产，乙方应以善良管理人的注意义务采取有效的措施保护该机密资料及密码，且乙方于任职期间或离职后均不以任何方式泄露或将该机密资料及密码交付给第三人。

2、乙方了解甲方所有电脑及其软件使用管理等信息（包括电脑数量、品牌、软件套数、名称、使用状况等）均系甲方之经营秘密，属乙方应保密范围，乙方应以善良管理人的注意义务采取一切适当措

施保管之，未经甲方事先同意不得以任何方式提供或泄露予任何第三方（包括甲方内部其它无关员工以及甲方外部人员等）。未经甲方事前书面同意不得私自复制、备份或以任何方式私自或为他人留存电脑所安装之任何软件（包括系统软件及应用软件等）。

3、乙方了解甲方设有专门的对外发言及信息披露制度，乙方承诺严格遵守该发言及信息披露制度。乙方了解在甲方依法公布或披露甲方任何营运信息前，乙方不得擅自向第三人告知、传播或提供有关甲方的任何机密资料。

4、乙方同意甲方对商业秘密之定义和界定，无论故意或过失、无论以任何形式泄露甲方商业秘密均属违约或违法行为（含犯罪行为），甲方有权视情节和危害程度，采取对商业秘密保护措施，并要求赔偿相关损失。乙方亦同意配合甲方调查，包括但不限于问话、交待事件过程、交付或保存事件相关资料及设备，同意甲方将存储资料、电脑邮件等封存、保全，根据甲方立场配合甲方进行控告和调查。

5、乙方确认知晓甲方薪资保密的相关规定并承诺严格遵守执行，不告知别人自己的薪资、奖金收入及发放情况，不探听、议论、盗取、阅览别人薪资、奖金之相关情况和资料。

6、乙方了解甲方设有诚信廉洁相关规约，乙方应严格遵守，即不向甲方交易对象（包括协力厂商、客户、供货商或服务商等，且无论交易是否成交）约定或索取任何不正当利益，包括回扣、佣金、不当馈赠或招待等。

7、乙方承诺于任职期间或离职后不为自己或他人之利益，唆使或利诱甲方及其关联企业员工离职或违背职务。

8、乙方承诺不进行贪污、挪用、侵占、盗窃甲方资金或财产或侵犯商业秘密之行为。

9、乙方承诺，未经事先披露并经同意，应要求乙方承担违约责任。

第九条 知识产权条款

不论以明示或默示方式，甲方应该对所披露信息享有所有权或其他权利，保证未侵犯第三方的知识产权，如乙方因使用甲方的信息损害了第三人的权利，则乙方应立即停止使用该信息，并且由甲方赔偿第三方的损失，乙方不构成违约，此情形仅限于乙方因工作需要而正当使用该信息。

第十条 通知规则

1、一方在本协议履行过程中向另一方发出或者提供的所有通知、文件、文书、资料等，均以本协议所列明的地址送达，一方向另一方手机或电子邮箱发送的短信或电子邮件亦视为已送达另一方。

2、如一方迁址、变更电话、电邮，应当书面通知另一方，未履行书面通知义务的，一方按原地址邮寄相关材料或通知相关信息即视为已履行送达义务。当面交付上述材料的，在交付之时视为送达；以邮寄、短信、电邮方式交付的，寄出、发出或者投邮后即视为送达。

第十一条 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、合作或合资之前，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。

第十二条 信息载体

1、乙方同意，乙方所持有或保管的记录着甲方保密信息的一切载体均归甲方所有。前述载体包括但不限于设备、光盘、磁盘、磁带、笔记本、文件、备忘录、报告、案卷、样品、账簿、信件、清单、软件程序、录像带、幻灯片或其他书面、图示记录等。乙方应当于离职时，或于甲方提出要求时，将前述载体交付给甲方。

2、若载体是由乙方自备的，且保密信息可以从载体上消除或复制出来，甲方有权随时要求乙方将保密信息复制到甲方享有所有权的其他载体上，并把原载体上的保密信息消除，否则视为乙方已同意将这些载体的所有权转让给甲方，甲方有权不予以返还该载体，但须向乙方支付该载体经济价值相对应的费用补偿。

第十三条 违约责任

1、乙方违反本协议任何保密义务（包括但不限于保密义务、禁止引诱与招揽义务，下同）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。双方约定，本协议项下之违约金（以下简称“违约金”），其违约金数额相当于乙方解除或者终止劳动合同前____个月（不足12个月的按折合成12个月的标准计算）核定工资与奖金总和的_____%。若甲方曾向乙方支付保密费的，在乙方违反本协议约定之保密义务时，除支付上述违约金外，乙方还应将甲方已经累计支付的保密费全部退还给甲方。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之约定要求乙方承担相应的违约责任，或根据有关法律、法规之规定要求乙方承担相应的侵权责任。

2、为便于计算乙方违约/侵权行为给甲方造成的损失，双方进一步约定，因乙方如下行为造成甲方实际损失的计算标准如下：

（1）乙方违反本协议约定，泄露、倒卖甲方客户信息及/或接触、鼓动、劝说、引诱或招揽甲方客户停止入金、进行出金、至其他甲方开户或解除与甲方的交易协议等造成甲方损失的计算公式：

甲方损失=[涉及甲方客户数量×(甲方单一客户开发成本+甲方单一客户年度平均交易手续费)]

（2）乙方违反本协议约定，接触、鼓动、劝说、引诱或招揽甲方员工从甲方离职去其他甲方或实体工作或提供服务，造成甲方损失的计算公式：

甲方损失=[涉及甲方客户数量×(甲方单一员工招聘成本+甲方单一员工的年度平均工资)]

（3）在任何情况下，若甲方实际损失根据上述标准计算出来的金额或根据其他标准计算出来的金额少于本协议约定的违约金标准的，则双方同意根据本协议约定的违约金标准作为认定甲方实际损失的依据。

第十四条 免责事由

如任何政府部门要求乙方披露保密信息，乙方应及时给予甲方书面通知，足以使甲方能够寻求保护

或其他适当的救济。如甲方没有获得保护或救济，或丧失取得保护或救济的权利，乙方应仅在法律要求的范围内向政府部门披露相关保密信息，并且应尽合理措施根据甲方的要求对保密信息进行任何修改，并为披露的任何保密信息取得保密待遇。

第十五条 保密费

本协议保密费为：_____,保密费从___年___月___日开始，按月支付，由甲方于每月的___日通过乙方的银行账户支付。乙方银行账户如下：

开户名称：_____

银行账号：_____

开 户 行：_____

第十六条 合同的解除

1、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。

第十七条 纠纷解决程序与管辖

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

（1）向本协议签订地人民法院提请诉讼；

（2）向_____仲裁委员会申请仲裁。

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

第十八条 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。

（以下无正文）

甲 方：_____（盖章） 乙 方：_____

法定代表人/授权代表:_____

日 期：_____ 日 期：_____

A.4　不侵犯商业秘密承诺函（参考文本）

承诺人姓名：

身份证号码：

鉴于本人在入职公司前接触过第三方的商业秘密，为避免因此可能产生的纠纷给公司造成不应有的损失，特此承诺如下：

一、本人完全知悉并遵守与任何第三方之间的关于商业秘密保护的法定或约定之义务，尊重第三方合法享有的商业秘密等知识产权。

二、本人未以不正当手段获取第三方的商业秘密，未经授权不会披露、使用或允许他人使用第三方的商业秘密。包括但不限于：不携带第三方商业秘密信息载体进入公司办公场所；不使用公司设备存储第三方商业秘密信息；不通过公司网络、通讯工具传输第三方商业秘密信息；工作中不使用第三方商业秘密信息。

四、本人不会以任何形式侵害第三方的技术秘密自行申请专利，或将第三方的技术秘密提供给公司用于申请专利。

五、如因本人侵害第三方的商业秘密产生的法律责任由本人自行承担。如因本人侵害第三方商业秘密对公司造成损失的，由本人向公司赔偿相应损失。

----------（以下无正文）----------

承诺人：

年　月　日

A.5 商务合作保密协议（参考文本）

甲　方：_____

法定代表人：_____ 统一社会信用代码：_____

电　话：_____　　传　真:_____

地　址：_____

项目联系人、电话及邮箱：_____

乙　方:_____

法定代表人：_____ 统一社会信用代码：_____

电　话：_____　　传　真：_____

地　址：_____

项目联系人、电话及邮箱：_____

甲乙双方正在就_____事项进行商务合作，双方在谈判或合作期间，均因合作需要可能接触或掌握对方有价值的保密信息（包括但不限于口头、书面或其他任何形式），双方本着平等自愿、协商一致、诚实守信的原则，为保护双方商业秘密事宜，于_____年__月__日（以下简称“生效日”），在中华人民共和国_____（具体签署地址），签署本保密协议以共同执行：

第一条 术语定义

本协议所称保密信息，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。

第二条 保密信息的范围

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

（1）双方的客户、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（移动和固定电话）、电子邮件地址、即时通讯方式或社交网络地址（QQ、MSN、Skype、微信、易信、来往、Line、微博、空间等）、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）双方经营活动有关的合同文本及法律文书；

（3）双方经营活动中涉及的关键价格信息；

（4）双方谈判或合作履约中的会议决议、会议纪要、谈判与磋商细节等资料；

（5）双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）；

（6）与双方资产、财务有关的信息（如存货、现金等资产的存放地、保险箱密码、数量、价值等，以及财务报表、账簿、凭证等）；

（7）双方的知识产权、专有技术等信息（如产品设计、产品图纸、生产制造工艺及技术、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）；

（8）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。

第三条 保密信息的例外

1、在披露时或披露前，已为公众所知晓的信息或资料；

2、能证明获得相关信息时已经熟知的资料或信息；

3、由第三方合法提供给乙方的资料或信息；

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

第四条 双方权利义务

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

2、如谈判、合作项目不再继续进行，或相关合同解除、终止，一方有权在任何时候向另一方提出返还、销毁保密信息的书面要求，另一方应按要求在_____个工作日内向对方返还、销毁其占有的或控制的全部保密信息，包括但不限于保密信息的全部文件和其它材料，并保证不留有任何复制版本。

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

第五条 保密义务期限

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

第六条 知识产权

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

第七条 保密信息的保存和使用

1、任何一方均有权在双方合作期间保存必要的保密信息，以履行约定义务。

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

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

第八条 违约责任

1、任何一方如违反本协议下的保密义务，应承担违约责任。双方约定，本协议项下之违约金（以下简称“违约金”），其违约金数额相当于双方拟达成或已达成合作金额的_____%。如本条款约定的上

述违约金不足以弥补因违反保密义务而给受害方造成的损失，受害方有权进一步向侵权方主张损失赔偿。

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

3、损失赔偿的范围包括但不限于以下费用：

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

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

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

第九条 适用法律和争议解决

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

（1）向本合同签订地人民法院提请诉讼；

（2）向_____仲裁委员会申请仲裁。

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

第十条 其他

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

2、本协议一式___份，双方各执___份，具有同等法律效力。

（以下无正文）

甲　方：_____（盖章）　　乙　方：_____

法定代表人/授权代表:_____　　法定代表人/授权代表:_____

日　期：_____　　日　期：_____

附 录 B
（参考性）
商业秘密制度检查表及典型泄密案例库

B.1 商业秘密制度检查表

企业商业秘密制度检查范围的参考内容见表 B.1。

表 B.1 企业商业秘密管理检查表

编号	标准模块	检查内容	检查结果
商业秘密管理组织			
1.1	企业负责人及高管保密意识	企业最高负责人有无发布要求保护商业秘密的讲话或相关文件？	☐ 有 ☐ 无
商业秘密管理制度			
2.1	制度建设	企业已制定、发布的商业秘密管理制度或文件中是否包含商业秘密管理的目标、方针、适用范围？	☐ 包含 ☐ 未包含
		有无关于公司商业秘密管理组织架构及职责分工的文件？	☐ 有 ☐ 无
		企业现行的商业秘密管理制度或文件中是否覆盖以下全部内容？ 商业秘密信息的识别与分级； 涉密物品管理； 涉密载体管理； 涉密纸质文档管理； 涉密计算机管理； 涉密网络管理； 涉密区域管理； 涉密人员管理； 泄密事件管理； 奖惩管理。	☐ 是 ☐ 否，已制定的文件包括__ _____ _____ _____ _____
商业秘密信息管理			
3.1	定密与分级	企业目前是否能够识别自身的商业秘密？	☐ 能够识别全部商业秘密 ☐ 能够识别大部分商业秘密 ☐ 无法识别商业秘密
		企业目前有无建立商业秘密信息的资产盘点制度？	☐ 形成有企业商业秘密信息清单或商业秘密信息资产盘点表 ☐ 对已形成的商业秘密信息清单或商业秘密信息资产

			实施了分级管理 ☐ 没有对企业的商业秘密信息进行盘点和形成清单
		企业目前是否有对商业秘密信息资料清单实施动态更新和管理？	☐ 有
			☐ 无
3.2	信息保密要求	涉密信息、涉密载体有无专人保管；有无采取保密措施？	☐ 有
			☐ 无
		涉密信息、涉密载体的对外流转、备份、复制、发布等，是否设置有内部审批流程？	☐ 是
			☐ 否
		是否对涉密信息、涉密载体的接触人员和接触权限进行限制？	☐ 是
			☐ 否
		如果发生商业秘密泄密事件，有无可以追溯涉案信息的产生、流转、复制、解密、销毁等过程的记录？	☐ 有
			☐ 无
		对于需要销毁的涉密信息采取了何种措施？	☐ 未采取措施 ☐ 碎纸机粉碎 ☐ 硬盘、U 盘格式化或消磁 ☐ 其他_____
员工管理			
4.1	涉密岗位识别	企业目前有无区分涉密岗位？	☐ 有区分涉密岗位和非涉密岗位
			☐ 有区分核心涉密岗位、涉密岗位和非涉密岗位
			☐ 没有
4.2	保密文化建设	企业有无开展线上、线下的保密教育培训？	☐ 有
			☐ 无
		企业目前开展保密教育培训针对的主要对象？	☐ 新入职员工 ☐ 全体员工 ☐ 重点或涉密岗位员工
		企业目前开展的保密宣传包括？	☐ 向员工推送宣传案例 ☐ 组织答题竞赛 ☐ 在办公场所内张贴宣传标语、播放宣传视频 ☐ 召开全员保密动员大会 ☐ 其他_____
		企业目前有无对员工进行商业秘密保护知识考核？	☐ 有
			☐ 无
4.3	履职管理	涉密员工能否识别大部分商业秘密和清楚保密要求？	☐ 能
			☐ 否
			☐ 不清楚
		目前企业员工参加的工作会议等活动涉及商业秘密的，有无采取保密措施？	有采取以下措施： ☐ 在涉密区域内召开

			☐ 使用保密会议室 ☐ 参加会议的员工应具备接触所涉商业秘密的权限或经审批 ☐ 告知其保密要求或签署保密承诺 ☐ 限制使用手机、便携机或拍摄、录音设备，使用防录音装置 ☐ 重要涉密纸质文档做好标识，会议后检查并回收 ☐ 采取会议密码、屏幕水印等保密措施 ☐ 其他_____
			☐ 无
外部人员管理			
5.1	临时来访人员管理	企业目前对临时来访人员有无采取管理措施？	有采取以下措施： ☐ 进行身份登记 ☐ 特定涉密区域限制设备使用 ☐ 涉密区域的专人陪同 ☐ 其他_____
			☐ 无
5.2	中短期涉密商务合作人员管理	企业目前对第三方专业服务等中短期商务合作人员有无采取管理措施？	有采取以下措施： ☐ 签署保密协议 ☐ 登记身份并佩戴不同颜色身份卡，限制进入非授权区域 ☐ 配备专用涉密电脑，限制拍摄设备使用 ☐ 其他_____
			☐ 无
5.3	长期涉密商务合作人员管理	企业目前对供应商、外部研发企业等长期商业合作人员有无采取管理措施？	有采取以下措施： ☐ 与外部企业签署保密协议 ☐ 要求参与项目的外部企业员工签署保密承诺 ☐ 登记身份并佩戴不同颜色身份卡，限制进入非授权区域 ☐ 使用企业提供的加密存储介质、网络或设备 ☐ 对外部人员使用的便携机等设备进行检查 ☐ 其他_____

			☐ 无
区域管理			
6.1	区域分级	企业目前对涉密物理区域采取何种管理措施？	有采取以下措施： ☐ 根据涉密区域重要程度采取物理隔离措施（如使用独立、封闭的办公区域） ☐ 设置有独立门禁、监控摄像头等 ☐ 张贴有禁止或警示标识 ☐ 配备安保人员和安保设备 ☐ 对涉密区域进行分级 ☐ 其他_____
			☐ 无
6.2		企业目前对网络区域有无划分？	☐ 有
			☐ 无
6.3	区域保密措施	目前企业最高涉密部门或重要涉密部门办公区域是否有与其他区域物理隔离？	☐ 是
			☐ 否
		目前企业对涉密网络采取了何种保密措施？	有采取以下措施： ☐ 独立网络 ☐ 区分内外网，涉密网络不接入外网 ☐ 启用终端准入、身份识别等安全验证技术 ☐ 网关启用安全监控 ☐ 其他_____
			☐ 无
设备及物品管理			
7.1	计算机	目前企业对涉密的计算机采取何种管理措施？	有采取以下措施： ☐ 涉密计算机使用账户口令、身份认证、访问控制、数据加密等安全措施 ☐ 限制非授权软件的安装 ☐ 限制接入非授权网络涉密 ☐ 计算机使用桌面云，工作数据上传至云端，不存储在本地 ☐ 限制/禁止移动存储接入 ☐ 限制/禁止涉密区域使用便携机办公 ☐ 其他_____

			☐ 无
7.2	手机	目前企业对智能手机采取何种管理措施？	有采取以下措施： ☐ 最高涉密区域非授权禁止使用私人智能手机 ☐ 私人智能手机禁止接入公司涉密网络或涉密信息系统，禁止拍摄涉密信息 ☐ 私人智能手机禁止存储工作数据 ☐ 私人智能手机限制使用工作软件 ☐ 其他_____
			☐ 无
7.3	纸质文档	目前企业对涉密的纸质文档采取何种管理措施？	有采取以下措施： ☐ 使用碎纸机粉碎废弃纸质文档 ☐ 专人管理涉密纸质文档并保留记录 ☐ 打印系统配备权限管理功能 ☐ 打印系统配备记录、备份管理系统 ☐ 其他_____
			☐ 无
7.4	物品	目前企业对载有涉密信息的产品、半成品、原料等物品有无采取管理措施？	有采取以下措施： ☐ 携带涉密物品外出时采取包装、密封等保密措施 ☐ 专人管理 ☐ 使用登记 ☐ 标签、物料或成分种类编制企业内部的编码统一管理 ☐ 其他_____
			☐ 无
7.5	移动存储介质	目前企业对载有涉密信息的移动存储介质有无采取管理措施？	有采取以下措施： ☐ 经审批才可使用移动存储设备 ☐ 移动存储设备未经允许不得链接非涉密电子设备 ☐ 使用移动存储介质存储涉密信息采取身份识别、内容加密、设备绑定等措施 ☐ 专人专管授权使用的移动存储介质 ☐ 其他_____
			☐ 无

信息系统及软件管理			
8.1	信息系统账号及口令、权限	目前企业有无对内部使用的信息系统采取管理措施？	有采取以下措施： ☐ 系统设置有登录密码、定时密码 ☐ 系统包括屏幕保护功能、屏幕水印、复制粘贴限制等保密措施。 ☐ 账号的设置、审批符合保密规定 ☐ 口令的设置、更换等符合保密规定 ☐ 涉密的软件和信息系统具备权限管理功能 ☐ 发生权限到期、人员变动、项目变更等情况时，及时收回或重新授权 ☐ 特别授权需经审批 ☐ 其他_____ ☐ 无
8.2	邮箱	目前企业有无对员工使用的邮箱采取管理措施？	有采取以下措施： ☐ 仅允许使用企业邮箱，禁用非企业邮箱地址，因工作需要使用个人邮箱应经审批 ☐ 邮箱内容备份超过 6 个月，核心岗位员工邮箱备份超过 12 个月 ☐ 使用的企业邮箱具备关键字过滤、外发邮件审批、邮件审计等保密功能 ☐ 其他_____ ☐ 无
8.3	通讯软件	目前企业有无对员工内部使用的即时通讯软件采取管理措施？	有采取以下措施：（采用的即时通讯软件 为_____） ☐ 内部使用的即时通讯软件避免和其他外部及时通讯软件进行内容的互通互联 ☐ 内部使用的即时通讯软件可以实现对用户登录进行网络、设备控制，保证安全环境下运行 ☐ 企业内部使用的即时通讯软件具备对聊天内容进行审计的后台监控管理功能 ☐ 企业内部使用的即时通讯软件在移动终端应具备禁止复制、转发、下载和全场

			景添加水印的管控功能 ☐ 其他_____
			☐ 无
8.4	网盘	目前企业有无对员工使用网盘采取管理措施？	有采取以下措施： ☐ 禁止/限制使用网盘，使用需审批 ☐ 对因工作需要经审批同意登录网盘的，固定 IP 或者固定电脑 MAC 地址访问，并将网盘账号和密码在企业内部备案管理 ☐ 其他_____
			☐ 无
8.5	网站	目前企业有无对员工登录网站采取管理措施？	有采取以下措施： ☐ 采取了白名单管理策略，仅允许员工登录工作需要的网站 ☐ 禁止访问允许上传文件的网站 ☐ 禁止/限制登录网页邮箱，登录需审批 ☐ 其他_____
			☐ 无
评估与改进			
9.1	检查	企业目前是否会定期或不定期对商业秘密管理工作的执行情况进行检查？	☐ 定期检查 ☐ 不定期检查
			☐ 没有进行检查
		企业对商业秘密管理工作执行情况的检查频次？	☐ 至少每月检查 1 次，并留存检查记录 ☐ 至少每季度检查 1 次，并留存检查记录 ☐ 至少每半年检查 1 次，并留存检查记录 ☐ 至少每年检查 1 次，并留存检查记录
9.2	评估	企业目前有无定期对商业秘密管理体系运行情况及问题进行总结、评估？	☐ 有
			☐ 无
9.3	改进	企业目前有无针对检查发现的问题制定改进计划，并跟踪改进情况？	☐ 有
			☐ 无
商业秘密泄露事件管理			
10.1	内部管理	企业目前有无指定内部受理商业秘密泄密事	☐ 有

		件报告窗口的负责人？	☐ 无
			☐ 有 ☐ 无
		企业目前有无制定内部泄密事件的分级标准、处理流程和应对预案？	☐ 有
			☐ 无
10.2	证据固定	企业目前有无制定发生泄密事件时的证据固定指引？	☐ 有
			☐ 无
10.3	外部维权	发生泄密事件时，是否能自行或寻求第三方专业机构启动法律手段维权？	☐ 是
			☐ 否

B.2 人工智能产业生成合成（深度合成）算法典型泄密案例库

B.2.1 郭某侵犯商业秘密案

案号：（2024）沪 0115 刑初 493 号

案情简介：

两被害单位绍兴某科技有限公司、上海某科技有限公司系母子公司，共同从事人工智能处理器 NPU 芯片的研发及销售，并于 2020 年 8 月研发完成涉案芯片项目。该项目芯片由多模块组成，其中涉案两项技术系自研模块，是实现芯片功能的关键技术。经鉴定，该两项技术信息在案发前不为公众所知悉。同时，被害单位通过对服务器设置物理隔离、控制网络访问及数据传输、制定保密工作制度、签署保密协议等，对涉案技术信息采取了相应保密措施。

被告人郭某原系被害单位创始人，并担任被害单位上海某科技有限公司首席运营官，负责涉案项目的芯片研发相关工作，并与被害单位签订了保密协议。2022 年 9 月至 11 月，被告人郭某因与被害单位其他创始人产生矛盾，为在后续与公司谈判时增加筹码和话语权，并便于离职后使用相关数据，在未告知其他股东的情况下，利用其任职所掌握的 root 账户权限，多次绕开服务器安全管理设置，擅自将包括涉案两项技术信息在内的大量保密数据非法复制、传输至本地电脑后上传至其个人网盘。此外，2022 年 8 月起，被告人郭某以案外公司核心人员身份参与该公司对外融资活动并出现在该公司大算力芯片项目宣传资料中。

经鉴定，被告人郭某上传至其个人存储空间的文件中所包含代码与涉案技术信息代码具有同一性。经评估，涉案两项技术信息的合理许可使用费为 231 万元。

2022 年 11 月，被告人郭某通过上述方式非法复制、传输保密数据时被公司当场发现并报警。2023 年 11 月，被告人郭某经公安机关电话通知后到案。其到案后承认其从两被害单位处复制、传输了核心数据至其个人网盘，但辩称其目的系为两被害单位备份数据，至检察机关审查逮捕时才如实供述上述基本犯罪事实。

判决结果：

上海市浦东新区人民法院于 2024 年 4 月 16 日作出（2024）沪 0115 刑初 493 号刑事判决：被告人郭某犯侵犯商业秘密罪，判处有期徒刑二年，缓刑二年，并处罚金十万元。一审宣判后，被告人未上诉、公诉机关未抗诉，判决已发生法律效力。

合规建议：

企业宜对核心技术人员实施最小权限原则，严格管控 root 等高权限账户，并部署技术防控措施，包括网络行为审计、异常数据传输监控、外发文件水印标记等，以便及时发现文件加密和上传等异常情况。

B.2.2 深圳市智某信息技术有限公司与光某（深圳）智能有限公司侵犯商业秘密纠纷案

案号：（2021）粤 03 民初 3843 号

案情简介：

原告深圳市智某技术有限公司系一家互联网高科技公司，主要业务为大数据智能挖掘技术应用与移动互联网客户端开发，主要产品有“天某”手机 APP，采用其自主开发的大数据追踪系统，进行智能跟踪、个性化推荐、智能摘要等，为企业提供“商业情报收集”和“舆情检测跟踪”服务。被告也是一家移动互联网公司，其开发的“学某某”APP 采用了与原告实质性相同的智能检索算法，为用户推荐全面、快速、清晰分类的兴趣学习课程推荐信息。

广东省深圳市中级人民法院认为，案涉智能检索算法本质是一种算法推荐，原告已通过签订保密协议或者在劳动合同中约定保密义务对涉案技术信息采取合理保密措施；涉案算法可提供更为精准的检索信息，为原告带来商业收益和可保持竞争优势，算法核心为模型的选择优化以及模型之间排除相互妨碍，达到最佳的制动效果，并不为公众所知悉且具有商业价值，相关技术信息符合认定为商业秘密法定条件。两家公司的研发团队成员有重合，被告对搜索算法构成实质性相同没有提出合理抗辩理由。被告“学某某”APP 中使用的被诉侵权搜索算法与原告请求保护的搜索算法构成实质相同，且其有渠道、有机会获得原告的案涉商业秘密。

判决结果：

广东省深圳市中级人民法院判决被告立即停止侵犯商业秘密的行为，下架侵权 APP 产品，并赔偿原告经济损失及合理维权费用共计人民币 20 万元。

合规建议：

企业宜对接触核心算法的研发人员实施分级授权管理，签订竞业限制协议，并对离职研发人员的工作设备进行数据清理核查，保留完整的算法开发文档作为权属证明。同时，企业可对核心算法实施代码混淆、分段加密等技术保护措施，建立从开发环境到生产环境的全流程访问日志，以便监测和追溯异常行为。

B.2.3 某网络科技公司诉浙江某兴信息技术公司、浙江某石信息技术公司侵害技术秘密纠纷案

案号：（2021）最高法知民终 2298 号

案情简介：

原告某网络科技公司为涉案软件源代码的权利人，并对该技术秘密采取了保密措施。某网络科技公司与浙江某兴信息技术公司签订的许可使用合同约定了许可费及许可期限，并明确约定了浙江某兴信息技术公司应当承担保密义务。2018 年 12 月 31 日，涉案软件源代码被披露至某共享平台，所披露代码中存在多个指向浙江某兴信息技术公司、浙江某石信息技术公司的信息，其中部分信息为仅由浙江某兴信息技术公司自身掌控的参数信息。浙江某石信息技术公司是浙江某兴信息技术公司的唯一股东。

最高人民法院经审理认为，涉案软件源代码构成技术秘密，浙江某兴信息技术公司披露涉案软件源代码的行为构成技术秘密侵害，应承担赔偿责任。在被诉侵权行为发生时，浙江某石信息技术公司是浙江某兴信息技术公司的唯一股东，其未提交二者财务独立的证据，不能证明浙江某兴信息技术公司的财产独立于自己的财产，依法应对浙江某兴信息技术公司的债务承担连带责任。

判决结果：

最高人民法院驳回上诉，维持原判。广东省深圳市中级人民法院一审判决两被告连带赔偿原告经济损失及合理维权费用共计 500 万元。

合规建议：

企业宜在技术许可合同中细化保密条款，明确约定被许可方的保密义务范围、保密期限、使用限制及违约责任，并对许可使用的技术秘密采取技术性保护措施，包括但不限于代码混淆、分段授权、数字水印等技术手段，以追溯泄密源头。

参 考 文 献

［1］ 全国人民代表大会.中华人民共和国反不正当竞争法.2019年
［2］ 最高人民法院.最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定：法释（2020）7号.2020年
［3］ 最高人民法院.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：法释（2025）5号.2025年
［4］ 最高人民检察院.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：高检法（2020）15号.2020年
［5］ 国家互联网信息办公室.互联网信息服务深度合成管理规定：国家互联网信息办公室 工业和信息化部 公安部令第12号.2022年
［6］国家互联网信息办公室.人工智能生成合成内容标识办法：国信办通字（2025）2号.2025年