ICS 03 100
CCS A 01

T/AIIA

团 体 标 准

T/AIIA 015—2025

具身智能机器人商业秘密保护指南

Guidelines for Trade Secret Protection of Embodied Intelligent Robots

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

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、中国质量认证中心有限公司、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、深圳逐际动力科技有限公司、深圳市优必选科技股份有限公司、源升智能机器人（深圳）有限公司、泰和泰（深圳）律师事务所、浙江垦丁（深圳）律师事务所、深圳市酷开网络科技股份有限公司、深圳市沃呈网络科技有限公司、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、曾云鹏、张景平、申晴、张康康、范丛明、梁乔玲、刘大亮、秦雨歌、姚莉芬、崔青青、陈泽加、郑美惠。

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具身智能机器人等重点发展方向，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。

在人工智能领域，具身智能机器人凭借独特的技术特点和广泛的应用场景，正逐步成为企业核心竞争力的重要组成部分。这类技术高度依赖于硬件设备和实时控制系统，其商业秘密保护需求集中于控制算法的安全管理、硬件设计防护及设备运维保密管理等方面。然而，随着相关产业的持续蓬勃发展，商业秘密的保护问题也日益凸显。相关商业秘密的泄露，不仅会导致企业技术优势丧失，还可能引发法律风险和商业受损，直接威胁企业的生存与发展。

在此背景下，本文件旨在为具身机器人产业的商业秘密保护提供参考，企业宜结合具身智能机器人产业特点，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、销售、采购、财务、人事、行政、商业合作等，并按照 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。

具身智能机器人商业秘密保护指南

1 范围

本文件提出了具身智能机器人产业商业秘密管理的总体要求，涉及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、供应链上下游、物理区域、物品及载体、信息系统、算法模型安全、云端安全、数据、泄密事件以及评估、审计和改进的管理要求。

本文件适用于具身智能机器人研发、生产、销售的企业或组织。事业单位、研究机构、协会等组织的商业秘密管理可参考本文件。不适用于已公开的技术方案保护。

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 12643-2013 机器人与机器人装备 词汇

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 36239-2018 特种机器人 术语

GB/T 41867-2022 信息技术 人工智能 术语

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 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

具身智能机器人 embodied intelligent robot

通过环境感知-决策-执行闭环系统实现物理交互的智能机器人，具备环境自适应及多模态交互能力。

注：包括但不限于人形机器人。

3.2

多模态交互 multimodal interaction

通过整合视觉、听觉、触觉等多种感知途径进行多模态输入，同时运用文本、音频、图像、动作等多种形式进行多模态输出，实现智能机器人与用户或环境间自然、流畅且高效信息交互的方式。

3.3

环境感知 environmental perception

通过各种传感器获取信息并处理，使智能机器人具备识别、判断自身及周边环境的状态的能力。

3.4

决策规划 decision planning

基于环境感知的信息或指令,完成特定任务解决方案和规划行动策略的能力。

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

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。

3.7

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）。

3.8

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。

3.9

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。

4 总体要求

4.1 概述

4.1.1 企业宜构建与具身机器人产业特点相匹配的商业秘密管理体系，覆盖具身机器人特有的本体运动控制技术、多模态感知融合框架、人机交互行为数据集及硬件仿制防护体系等核心领域，实现商业秘密保护与科技创新效率的协同发展。

4.1.2 企业的商业秘密管理工作应由企业最高管理者牵头，高管负责，专人管理，全员参与。

4.1.3 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。

4.1.4 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。

4.1.5 企业宜建立商业秘密保护与文化建设的联动机制，通过定期意识培训、典型案例警示、合规承诺书签署等方式，培育全员商业秘密保护文化。

4.1.6 企业商业秘密管理体系需与机器人产业技术迭代周期动态适配，建立技术生命周期与密级联动的评估机制。

注：如硬件设计周期、算法更新频率等。

4.1.7 企业宜建立商业秘密保护有效性评估制度，结合以下要素定期进行体系评审：

a) 技术形态演进评估，例如多模态感知系统、仿生运动控制算法、情境认知模型等技术迭代对保密范围的影响；

注：检查人机交互类算法由于技术开源社区发展调整密级的需要。

b) 供应链技术节点保密，例如审查精密执行器供应商、传感器融合方案外包方、云脑训练数据服务商等环节的保密协议执行情况；

c) 研发数据、训练数据的保密处理，例如具身学习训练数据集（含动作捕捉数据、环境交互日志）的脱敏处理有效性审查；

d) 员工流动风险再评估，例如关键岗位的竞业限制协议覆盖完整性、核心研发岗位离职后竞业履行情况再评估；

e) 商业秘密司法保护实践动态追踪：密切留意商业秘密司法保护领域的实践进展。

4.2 企业内部与外部商业秘密协同保护总体要求

4.2.1 企业宜构建内外协同的商业秘密保护体系，对内部研发数据与外部合作信息实施全生命周期加密管控，并建立完善的溯源追责体系。

4.2.2 企业宜严格规范商业秘密交互流程，在技术合作、供应链协同等外部合作中遵循最小必要信息共享原则，并建立常态化安全审计机制，定期对信息交互过程进行合规性检查。

4.2.3 企业宜建立商业秘密保护的内外联动响应机制，制定统一的保密标准与操作规范。

4.3 算法商业秘密保护总体要求

4.3.1 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。

4.3.2 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。

4.3.3 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。

4.4 数据商业秘密保护总体要求

4.4.1 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。

4.4.2 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。

4.4.3 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。

4.4.4 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。

4.5 代码商业秘密保护总体要求

4.5.1 企业代码商业秘密可能面临内部泄露、外部侵入、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。

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

4.5.3 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。

4.5.4 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。

4.6 硬件商业秘密保护总体要求

4.6.1 企业硬件商业秘密管理应严格执行最小接触原则、分段知悉原则、物理隔离原则、加密存储原则、痕迹留存原则。

4.6.2 企业宜针对硬件商业秘密保护进行涵盖研发阶段、生产阶段、供应链合作等环节的全生命周期管理。

4.6.3 企业宜针对核心硬件进行专项识别与分类分级，并将其纳入商业秘密保护体系，核心硬件包括但不限于具身智能机器人所属产业涉及到的关节，材料，传感器、减速器、伺服系统、控制器、电机等，以及与这些硬件对应的生产、测试、装配的流程、规范和数据等。

4.6.4 企业宜建立与具身机器人硬件特性相适应的商业秘密保护体系，确保硬件商业秘密保护与产品快速迭代的协同推进。

4.7 供应链商业秘密保护总体要求

4.7.1 企业宜构建供应链商业秘密防护体系，包括与供应商及相关保密义务人员签署保密协议（见附录 A.5）等，覆盖具身机器人核心零部件技术参数、供应商名录、精密生产工艺流程及质量管控标准等关键商业信息。

4.7.2 企业宜基于生产流程，对技术信息进行模块化拆解，对核心部件采取封装技术处理，降低信息泄露风险。同时，建立常态化供应商安全审计机制，定期评估合作方保密能力。

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 具身智能机器人企业宜评估并识别商业秘密信息，结合产业特点，按照研发设计、生产制造、测试应用、场景应用与运维环节等全流程进行商业秘密保护体系建设。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 具身智能机器人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 研发设计环节的商业秘密确定

5.2.1 概述

企业研发设计环节的商业秘密确定，宜覆盖研发设计全流程，涵盖需求分析与立项评估、系统架构设计、硬件设计、软件与算法开发、原型开发与测试等多方面内容，将立项评估报告、产品设计图纸等信息，纳入企业商业秘密保护范畴。

5.2.2 需求分析与立项评估

在需求分析与立项评估环节，企业宜将市场调研、立项评估报告、技术可行性分析等作为商业秘密。

5.2.3 系统架构设计

在系统架构设计环节，企业宜将功能模块划分、接口协议定义的具体方案作为商业秘密。

注：功能模块划分的具体方案包括感知模块设计（例如传感器方案设计与选型）、决策模块设计（例如算法框架设计，实现路径规划、任务调度的具体方式等）、执行模块设计（例如驱动系统设计方案等）。

5.2.4 硬件设计

在硬件设计环节，企业宜将围绕机械结构设计、电子电路设计相关的集成电路图纸、产品设计图纸、参数、代码、数据等作为商业秘密。

5.2.5 软件与算法开发

在软件与算法开发环节，企业宜将该设计过程中的感知算法、决策与控制算法、人机交互模型等作为商业秘密。

5.2.6 原型开发与测试

在原型开发与测试环节，企业宜将硬件原型组装方案、算法集成测试、测试场地设计方案、测试数据等作为商业秘密。

5.2.7 迭代优化与验证

在迭代优化与验证环节，企业宜将过程中涉及的调试文档、性能调优方案、安全合规验证等作为商业秘密。

5.2.8 其他研发环节

在其他研发环节，企业宜将过程中涉及的研发协作信息、跨学科融合研发成果等作为商业秘密。

5.3 生产制造环节的商业秘密确定

5.3.1 核心零部件制造

在核心零部件制造环节，企业宜将传感器、执行器等核心零部件制造过程中产生的图纸、工艺、配方、数据等作为商业秘密。

5.3.2 整机组装

在整机组装环节，企业宜将机械结构组装、电子系统集成等环节中涉及的参数调整、配方、信号时序配置、PCB布局设计、固件烧录密钥、加密协议等作为商业秘密。

5.3.3 生产制造环节调试与测试

针对生产制造环节调试与测试，企业宜将硬件调试、软件调试等作为商业秘密。

5.3.4 包装与供应链管理

在包装与供应链管理环节，企业宜将产品防护设计方案、物流追踪规则、零部件采购清单、生产排期策略等作为商业秘密。

注：如采用特定标签加密规则。

5.3.5 其他生产制造环节

在其他生产制造环节，企业宜将供应链协同数据、工艺参数优化方案等作为商业秘密。

5.4 测试评价环节的商业秘密确定

5.4.1 功能验证测试

在功能验证测试环节，企业宜将基础功能测试、算法逻辑验证、异常场景测试用例、原始测试数据等作为商业秘密。

5.4.2 性能评估测试

在性能评估测试环节，企业宜将运动性能测试、操作性能测试、能效测试、耐久性测试参数设置、原始测试数据等作为商业秘密。

5.4.3 安全与合规测试

在安全与合规测试环节，企业宜将安全功能验证、合规性验证方案、内部合规评审记录以及涉及这些内容的变更技术说明、文档、代码、数据等作为商业秘密。

5.4.4 其他测试环节

在其他测试环节，企业宜将测试报告与分析、测试环境配置、第三方测试协作信息、测试过程中的问题追踪与解决方案文档等作为商业秘密。

5.5 场景应用与运维环节的商业秘密确定

5.5.1 场景应用与运维环节

在场景应用与运维环节，企业宜根据产品使用场景，将不同场景下的测试内容、用户验收测试等作为商业秘密。

5.5.2 其他场景应用与运维环节

在其他场景应用与运维环节，企业宜将用户数据与交互信息、运维数据与诊断技术、场景适配与优化技术等作为商业秘密。

5.6 算法的商业秘密信息确定

5.6.1 算法研发与设计

在算法研发与设计环节，企业宜将运动控制算法、环境感知算法、决策规划算法逻辑、多模态融合算法框架及对应的架构、参数、训练策略、结果等作为商业秘密。

5.6.2 算法训练与优化

在算法训练与优化环节，企业宜将专用训练数据集构建方法、超参数调优方案、模型剪枝与量化技术、对抗样本防御策略、迁移学习应用技巧等作为商业秘密。

5.6.3 算法部署与运行

在算法部署与运行环节，企业宜将算法加密方案、实时推理加速技术、分布式计算调度策略、动态负载均衡方法、异常恢复机制等作为商业秘密。

5.6.4 其他算法相关环节

在其他算法相关环节，企业宜将算法测试与验证、算法更新与维护、算法安全与防逆向等其他算法相关信息作为商业秘密。

5.7 数据的商业秘密信息确定

5.7.1 数据采集、生成及产出

在数据采集、生成及产出环节，企业宜将多模态传感器数据融合规则、仿真数据生成算法、真实场景数据采集方案、数据标注质量控制标准、数据增强处理技术等作为商业秘密。

5.7.2 数据处理与分析

在数据处理与分析环节，企业宜将数据清洗流程、特征提取方法、异常数据检测规则、数据关联分析模型等作为商业秘密。

5.7.3 其他数据相关环节

在其他数据相关环节，企业宜将数据存储与管理设计、数据应用与价值挖掘方法、数据安全与合规方案等作为商业秘密。

5.8 代码的商业秘密信息确定

5.8.1 系统架构设计

在系统架构设计环节，企业宜将模块间通信协议、分布式计算框架设计、实时系统调度策略、容错机制实现代码、性能优化关键代码等作为商业秘密。

5.8.2 接口与集成

针对接口与集成环节，企业宜将硬件驱动层实现代码、第三方系统对接协议、API 安全验证机制、数据交换格式处理代码、系统集成测试套件等作为商业秘密。

5.8.3 测试验证代码

在测试验证代码环节，企业宜将测试框架代码、自动化测试脚本、性能基准测试工具、测试方案、设计及验证环境配置方案等作为商业秘密。

5.8.4 其他代码相关环节

在其他代码相关环节，企业宜将代码部署与运维方案、代码安全防护措施等作为商业秘密。

5.9 硬件的商业秘密信息确定

5.9.1 核心部件设计与制造

在核心部件设计与制造环节，企业宜将关节结构设计图纸、特种材料配方与处理工艺、传感器校准参数、减速器精密加工技术、伺服系统控制算法硬件实现等作为商业秘密。

5.9.2 系统集成与组装

在系统集成与组装环节，企业宜将机械-电子系统匹配参数、部件间接口规范、装配工艺流程、动态平衡调试数据、整机性能优化方案等作为商业秘密。

5.9.3 测试验证与质量控制

针对测试验证与质量控制环节，企业宜将耐久性测试方案、环境适应性测试数据、故障模式分析报告、质量检测标准体系、可靠性验证方法等作为商业秘密。

5.9.4 实训与调试数据

在实训与调试数据环节，企业宜将运动控制参数优化数据集、伺服系统响应特性曲线、关节负载测试记录、故障诊断知识库、实操培训专用案例库等作为商业秘密。

5.9.5 其他硬件相关环节

在其他硬件相关环节，企业宜将硬件安全防护技术、维护技术方案等作为商业秘密。

5.10 供应链的商业秘密信息确定

5.10.1 核心经营信息保护

在供应链核心经营信息保护环节，企业宜将采购成本核算模型、战略供应商评估体系、客户定制需求数据库、产能优化分配方案、物流成本控制策略等作为商业秘密。

5.10.2 供应商管理体系

在供应商管理体系环节，企业宜将合格供应商名录、供应商分级评定标准、采购谈判策略、供应链风险预警机制、替代供应商开发计划等作为商业秘密。

5.10.3 技术交付与协同

针对技术交付与协同环节，企业宜将外协加工技术规范、零部件验收测试标准、技术接口控制文档、协同开发保密协议、技术变更管理流程等作为商业秘密。

5.10.4 其他供应链相关环节

针对其他供应链相关环节，企业宜将智能仓储管理系统、成本优化技术等作为商业秘密。

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。

6.1.2 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载体上明确标识。

6.1.3 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。

6.1.4 对硬件研发涉及的 3D 设计图纸、电路板布线图等特殊载体，宜增设“动态密级”标识，当设计版本更新时触发密级复核流程。

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。

6.2.2 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。

6.2.4 针对机器人原型机等实体载体，宜建立“核心部件拆解保管”制度，将控制系统、驱动模块等关键部件拆分存储，配套使用区块链存证技术记录拆装过程。

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。

6.3.4 对跨国技术协作场景，宜使用企业定制版加密协作平台，具备屏幕水印、禁止截屏、地理围栏等数字版权管理（DRM）功能。

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。

6.4.3 企业宜对核心商业秘密资产采取分布式存储策略，将加密数据分块存储于多个物理隔离的安全存储节点，确保数据完整性与可用性。

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。

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。

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。解密保密文件宜由原登记部门评估确认，解密后的文件宜加盖“已解密”印章。

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。解密后的信息应及时回收并做相应处理。

注：如员工申请查看加密文件时，宜说明具体用途和使用时间，审批记录保存宜维持 2 年。

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。

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。

6.8.3 宜建立“硬件退役处理中心”，对机器人控制主板等含核心技术的报废部件，采用双重销毁确认机制。

6.9 文件管理

6.9.1 所有商业秘密信息的产生、保存、流转、复制、发布、解密、销毁等均宜保留记录。

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) 负责人机制：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，专职负责人需具备法律/信息安全专业背景，且不得兼任业务部门职务。也可由企业最高管理者直接负责商业秘密管理部门；
b) 管理人员配置：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) 总体框架：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) 组织架构：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) 管理部门职责：商业秘密管理部门的职责应包括商业秘密信息、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；

注：如结合具身智能特有的管理职责，围绕技术内核进行具身智能训练场数据隔离管理、物理交互指纹特征库的访问权限控制、开源代码库与私有代码库的隔离审查等；

f) 商业秘密管理部门应定期组织会议，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。

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，如编写《保密管理操作手册》等，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。

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，并保留相关记录存档。

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) 定期通过企业微信、飞书等在线即时通讯软件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，根据岗位涉密程度不同予以分层测试，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。

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应形成书面文件，

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 涉密人员离职前宜由企业法务部门或其他对接人员与之谈话，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。核心研发人员移交需由两名监交人签字确认。

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，宜及时收集并固定证据，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。

9.5 内部调动管理

9.5.1 跨部门调动宜重新评估密级权限。

注：如原岗位系统访问权限 6 小时内关闭。

9.5.2 涉密岗位平级调动宜签署《岗位保密责任变更确认书》，并进行备案。

9.5.3 核心技术人员调动前宜执行数据资产清查，交接记录由审计部复核存档。

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，如使用防窥膜遮挡显示屏、张贴“禁止拍摄”警示标识等。

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（见附录 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，可通过堡垒机采取保密措施。同时禁止使用个人邮箱传输涉密文件，统一使用企业加密邮件系统。

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) 使用企业提供的保密计算机；
c) 使用企业提供的加密系统；
d) 使用企业提供的加密存储介质；
e) 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 供应链上下游管理

11.1 供应商准入与分级管理

11.1.1 企业宜建立供应商准入白名单制度，对上游原材料、核心零部件供应商实施商业秘密保护能力审查。

11.1.2 企业宜根据供应商接触商业秘密的敏感程度分级，差异化签订保密协议（NDA）与责任条款。

注：如一级供应商：涉及算法定制化硬件；二级供应商：通用零部件。

11.2 技术材料交付管控

11.2.1 分段交付

硬件设计图纸、软件 SDK 等按生产阶段宜拆分交付，避免单一供应商掌握完整技术链路。

11.2.2 加密传输

技术文档宜采用算法加密，硬件固件通过安全芯片签名后传输。

11.2.3 交付验收

企业宜设立技术交付物“洁净交接区”，对供应商返还的样品、测试设备进行数据擦除验证。

11.3 商业秘密隔离与泄密追溯机制

11.3.1 概述

企业对上下游合作伙伴设置数据宜访问“防火墙”，例如仅向代工厂开放生产排期数据，屏蔽原材料成本明细，向供应商提供的经营数据需经脱敏处理。

11.3.2 物理标识嵌入

企业宜在硬件模组中植入激光微刻二维码或 RFID 芯片，实现部件级溯源。

11.3.3 数字水印技术

企业宜在交付的图纸、软件中嵌入隐形水印，泄露文件可通过水印 ID 定位泄密方。

11.3.4 联合追责条款

企业宜在合同中明确供应链各环节连带责任，要求供应商承诺承担其下级供应商泄密后果。

11.3.5 透明加解密技术

企业宜采用透明加解密技术对商业秘密实施动态保护，确保授权环境下自动解密使用，非授权环境仅显示加密内容。

11.4 上下游信息共享安全控制

11.4.1 共享平台管控

企业可基于区块链技术构建供应链协同管理平台，对包括但不限于设计变更、订单状态、交付进度等关键业务信息的全流程操作进行分布式存证，确保数据操作的不可篡改性与可追溯性。

11.4.2 最小授权原则

企业宜通过 RBAC（基于角色的访问控制）限制上下游企业查询权限，如仅允许物流商查看发货时间节点。

11.4.3 零信任原则

企业宜实施零信任原则，对上下游所有访问请求进行持续验证。

11.4.4 审计追踪

对第三方调用 API 接口的行为宜进行实时监控，异常访问触发自动告警。

注：如非工作时间高频下载。

12 物理区域管理

12.1 区域划分

企业内部的办公区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。涉密等级高的办公区域宜设置在离企业出入口相对较远的位置。

12.2 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并签署《保密承诺书》；
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。

12.3 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。

12.4 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。

12.5 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。

12.6 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，留存操作日志；

注：如操作日志保存 180 天。

h） 配备独立的网络基础设施。

注：如服务器、防火墙、专线等。

12.7 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。

13 物品及载体管理

13.1 计算机

13.1.1 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。

13.1.2 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。

13.1.3 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。

13.1.4 计算机未经批准不宜安装非授权软件。

13.1.5 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。

13.1.6 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。

13.2 智能手机

13.2.1 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应关闭或禁用摄像头、麦克风，不宜在涉密区域内拍摄、录音、设置热点。

13.2.2 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。

13.2.3 个人智能手机不宜接入企业涉密网络。

13.3 纸质文档

13.3.1 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。

13.3.2 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。

13.3.3 废弃的纸质文档宜通过碎纸机粉碎，不应随意丢弃。

13.4 产品

13.4.1　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。
13.4.2　涉密项目的不良品宜交由专人处理或报废，不宜随意丢弃。
13.4.3　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。

13.5　移动存储介质

13.5.1　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。
13.5.2　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。

14　信息系统管理

14.1　权限管理

14.1.1　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。
14.1.2　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。
14.1.3　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。
14.1.4　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。

14.2　账号及口令

14.2.1　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。
14.2.2　外部人员的账号宜与内部员工账号有明显的区别。
14.2.3　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。
14.2.4　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，且应规定修改口令设置的位数、更换周期的最低标准。
14.2.5　信息系统的口令宜通过系统设置强制用户定期更换。

14.3　信息出口控制

14.3.1　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。

14.3.2　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。
14.3.3　企业宜建立代理服务器访问备份系统，备份代理服务器访问日志。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。
注：如代理服务器访问日志备份 6 个月以上。
14.3.4　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。
14.3.5　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。

14.3.6 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。

14.4 保密措施

14.4.1 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。

14.4.2 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。

14.4.3 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。

14.4.4 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。

14.4.5 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。

14.4.6 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。

14.4.7 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。

14.4.8 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。

15 算法模型安全管理

15.1 模型访问控制

15.1.1 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。

注：如动态密钥更新周期≤72 小时；密钥分发采用特定算法加密；访问日志保存 180 天等。

15.1.2 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。密钥定期轮换，存储于硬件安全模块 HSM 中。

15.1.3 企业可采用云端部署模式实现模型运行与服务化，并采取分层加密、接口防护、全链路监控等安全控制措施。

15.2 防逆向保护

15.2.1 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。

15.2.2 具身智能模型参数和权重实施分段加密存储，不同模块采用独立密钥，并部署参数访问监控系统，记录异常访问行为。

15.2.3 模型部署包可嵌入数字水印，包含企业标识符，数字水印嵌入要求：

a） 水印不可见且抗篡改；

b） 每个部署包生成唯一水印；

c） 水印提取需专用工具；

d） 水印信息录入企业溯源系统。

15.2.4 宜实施分级访问控制，按需分配模型访问权限，并定期开展模型安全评估，检查防护措施有效

性。

16 云端安全管理

16.1 访问隔离

16.1.1 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。

16.1.2 API 调用宜绑定设备指纹，包含控制器序列号与安全芯片 ID。

注：如若设备连续 3 次认证失败或长时间未连接，需自动冻结 API 访问权限。

16.2 运维审计

16.2.1 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。日志文件禁止手动修改。

16.2.2 企业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。

16.3 云环境适配

16.3.1 企业宜要求云服务商提供 API 接口实现密钥自主托管。

16.3.2 多云存储场景下，企业宜实施碎片化加密存储。

17 数据管理

17.1 分级保护

17.1.1 企业宜根据本文件第 6.1 条建立数据保护分级体系。

17.1.2 企业宜明确不同密级数据的标识规则。

注：如颜色标记、数字水印、元数据标签。

17.2 生命周期管控

17.2.1 企业宜对数据进行全生命周期管控，具体包括以下方面：

a) 创建阶段：要求所有数据生成时标注创建者、用途及预期保密周期。

b) 存储阶段：核心数据必须采用硬件级加密，重要数据实施双重备份隔离存储。

c) 销毁阶段：建立覆盖物理销毁（碎纸/消磁）与数字擦除的验证机制。

17.2.2 企业宜实施最小化授权策略，权限分配宜经部门负责人与保密专员双审。

17.3 流转控制

17.3.1 内部流转规范

a) 企业宜建立专用数据总线，要求所有传输行为记录完整操作日志。

注：如包含时间戳、操作者 IP/MAC 地址等。

b) 企业宜设置异常流量预警阈值。

注：如单日数据导出量超过岗位均值 200%时触发审计。

17.3.2 外部交互管控

a) 企业宜强制使用安全沙箱技术处理第三方数据交换，禁止原始数据直接外发。

b) 企业宜对外提供测试数据需完成脱敏处理（包括结构脱敏与内容混淆）。

17.4 介质管理

17.4.1 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。

18 泄密事件管理

18.1 内部管理

18.1.1 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。

18.1.2 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) 立即封锁泄露渠道防止信息进一步扩散或损失扩大；

注：如禁用账号、断开网络等。

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。

18.2 证据固定

18.2.1 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。

18.2.2 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。

18.2.3 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。

18.3 外部维权

18.3.1 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。

18.3.2 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。

18.3.3 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。

18.3.4 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。

18.3.5　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。

18.3.6　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。

19　评估、审计与改进

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。

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　企业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。

18.5　持续监控要求

a）　企业宜部署用户行为分析（UEBA）系统，建立常见典型异常行为特征库（见附录 B.2）。

b）　季度穿透式审计宜覆盖数据创建、修改、流转全链条。

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
研发信息	设计图纸、模型、样板、方案、测试记录及数据、进度表等
生产信息	产品配方、工艺流程、技术参数、电子数据、作业指导书、样本库等
硬件信息	设备仪器的型号、配置参数、特别要求等
软件信息	源代码、应用程序、数据算法、模型参数信息和权重等
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
经营信息	采购计划、采购记录、营销策划、营销方案等
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）
商业秘密制度自查表及异常行为特征库

B.1 商业秘密制度自查表

企业商业秘密制度检查范围的参考内容见表 B.1。

表 B.1 企业商业秘密管理自查表

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　具身机器人企业管理典型异常行为特征库

具身机器人企业管理典型异常行为特征库的参考内容见表B.2。

表 B.2　具身机器人企业管理典型异常行为特征库

企业管理环节	异常行为及异常值（具体参数仅供参考）
研发环节异常	**1. 训练数据异常外泄** • 特征：研发环境非授权设备接入频次突增 300% • 检测：网络流量 DPI 深度检测+设备指纹白名单校验 • 关联风险：生成式 AI 语料库非法提取 **2. 模型逆向工程攻击** • 特征：API 调用频率超基线值 5 倍且参数组合异常 • 检测：对抗样本注入测试+模型水印追踪技术
生产部署异常	**3. 固件非法篡改** • 特征：TPM 芯片度量值偏离基准±15% • 检测：可信启动链验证+运行时内存校验 **4. 传感器数据窃取** • 特征：IMU 陀螺仪数据周期性缺失 • 检测：多模态数据一致性校验（视觉-力觉-位觉）
运维交互异常	**5. 特权账户滥用** • 特征：维护人员单日数据导出量超岗位均值 20 倍 • 检测：基于角色的动态基线建模 **6. 物理攻击痕迹** • 特征：外壳完整性传感器连续 3 次告警 • 检测：微振动频谱分析+三维形变扫描
数据流通异常	**7. 模型参数泄露** • 特征：神经网络权重矩阵相似度>92% • 检测：联邦学习梯度混淆验证 **8. 供应链数据污染** • 特征：零部件供应商数据包哈希值突变 • 检测：区块链存证交叉验证
特殊场景异常	**9. 跨域关联攻击** • 特征：同一 IP 在研发测试与生产环境并发访问 • 检测：网络拓扑隔离度分析

	10. 生物特征滥用 • 特征：人脸识别数据用于非绑定场景 • 检测：多因子关联性验证（声纹+步态）

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