

团 体 标 准

T/SZS XXXX—XXXX

商业秘密资产运营指南

Guidelines for the operation of trade secret assets

2026-XX-XX 发布

2026-XX-XX 实施

深圳市深圳标准促进会 发布

目 次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 1

5 商业秘密资产运营基础 1

6 商业秘密资产识别与确认 2

7 商业秘密资产登记 3

8 商业秘密资产评估 3

9 商业秘密资产运营方式 4

10 商业秘密资产运营保护 6

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。

本文件由xxx提出。

本文件由深圳市深圳标准促进会归口。

本文件起草单位：。

本文件主要起草人：。

引 言

商业秘密作为企业核心竞争力的重要组成，其市场价值日益凸显，但当前相关标准多侧重“防御性管理”，缺乏对商业秘密资产转让、许可使用、作价入股等运营活动的系统性规范，导致企业面临权属界定模糊、运营路径不清晰等问题。为推动商业秘密从“静态保护”向“动态增值”转化，完善“保护—运营—维权”全链条体系，助力产业高质量发展，特制定本文件。

商业秘密资产运营指南

1 范围

本文件给出了商业秘密资产运营的基本原则、运营基础、商业秘密资产识别与确认、商业秘密登记、商业秘密资产评估、商业秘密资产运营方式、商业秘密资产运营保护的建议。

本文件适用于各类拥有商业秘密资产的企业、科研机构等组织开展商业秘密资产运营活动。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

3.1

商业秘密资产 trade secret assets

通过确认和有效保护，能够持续发挥作用并且为权利人带来经济利益的非公开商业信息权益。

3.2

商业秘密权益初步确权登记 registration of trade secret rights and interests preliminary confirmation

权益人对合法拥有的商业秘密，向第三方机构提出登记申请，并获取登记证书的行为。

3.3

商业秘密资产运营 trade secret asset operation

拥有商业秘密资产（3.1）的企业、科研机构等组织，在符合相关法律法规基础上，以联合研发、交易许可等方式推动价值转化，实现商业秘密资产从静态保护到动态增值的系统性活动。

4 基本原则

4.1 坚持“合规管理、依法运营、全程保护”，将商业秘密资产运营纳入组织整体发展战略，统筹商业秘密保护与价值转化工作。

4.2 最高管理者为商业秘密资产运营第一责任人，保障人力、物力、财力等资源投入。

4.3 在商业秘密资产运营的全生命周期开展安全保护，确保运营流程安全可控。

4.4 商业秘密资产运营宜平衡资产安全、运营效率与管理成本。

5 商业秘密资产运营基础

5.1 运营管理部门

5.1.1 商业秘密资产运营工作可依托有商业秘密管理职能的部门（如商业秘密管理、法务、人事、信息安全、知识产权等部门）开展，宜在原有保密体系基础上建立商业秘密资产运营体系，相关制度、人员架构宜视情况优化或共用。

5.1.2 运营管理部门职责包括但不限于：

- 商业秘密资产识别和管理；
- 商业秘密资产运营体系文件的制定、发布、实施和改进；
- 明确商业秘密资产运营管理部门成员的工作职责；
- 组织或指导开展商业秘密资产运营及相关宣传、培训工作；
- 监督、检查商业秘密资产运营制度的实施，并持续改进。

5.2 运营制度

5.2.1 运营管理部门宜制定、发布、实施和改进商业秘密资产运营的制度文件，包括但不限于：

- 商业秘密资产运营的目的、策略和原则；
- 商业秘密资产运营职责与分工；
- 商业秘密资产运营的培训；
- 商业秘密资产运营的责任与奖惩。

5.2.2 运营管理部门宜定期检查并依据检查结果、法律法规及企业经营变化，及时修订、完善商业秘密资产运营管理制度。

6 商业秘密资产识别与确认

6.1 运营管理部门宜指导各业务部门定期或按项目开展商业秘密资产识别工作。涉密部门负责人为该部门商业秘密资产识别第一责任人，保证商业秘密识别正确且完整地清查、记录与保存。

6.2 商业秘密资产的识别与确认的内容包括但不限于：

- 商业秘密的权益基础；
- 商业秘密保护重点与管理的范围；
- 商业秘密许可、转让、质押融资、作价入股等运营场景中的具体标的；
- 商业秘密鉴定或诉讼维权时的具体证据材料。

6.3 商业秘密资产确认的过程包含商业秘密载体盘点与归档。组织宜安排各涉密部门或专人落实商业秘密载体盘点。鉴于商业秘密载体清查盘点工作专业性较强，组织可委托具备相应资质的司法鉴定机构协同实施，但在司法鉴定机构进场开展工作前，需要签订第三方保密协议。

6.4 在条件允许的情况下，可组建由技术、法务、知识产权等相关负责人组成的商业秘密技术审查会，帮助识别与确认商业秘密资产。

6.5 商业秘密技术审查会对下列事项作出审查：

- 是否构成商业秘密；
- 密级、保密范围、保密期限；
- 核心密点、载体形式、保护方式；
- 是否适合运营及运营风险；
- 其他必要的审查事项。

6.6 商业秘密技术审查会可实行项目制或定期制，形成审查纪要与结论，作为商业秘密资产识别与确认的依据。

7 商业秘密资产登记

7.1 商业秘密资产存证

7.1.1 商业秘密资产登记前对商业秘密载体、商业秘密权利证明类及管理实施类文件等材料进行存证。

7.1.2 商业秘密资产存证宜优先采用不需要原文存证的电子数据存证方式，仅通过提交可代表商业秘密存证原件唯一识别值的哈希值来取得存证证明。

7.1.3 每次正式提交商业秘密存证原件前，宜确认电子数据存证平台的真实性、可靠性、完整性与可用性。

7.2 商业秘密资产登记

7.2.1 商业秘密资产登记可作为商业秘密资产价值评估、运营、维权举证的基础依据。

7.2.2 运营管理部门负责培训与指导各部门进行商业秘密资产登记申请。涉密部门主管为该部门商业秘密资产登记第一负责人，具体准备商业秘密资产登记材料。

7.2.3 商业秘密资产可以在组织内部自行登记，也可以向中立第三方机构申请商业秘密权益初步确权登记。针对企业重要的或有运营需求的商业秘密资产，宜在中立第三方进行登记。

7.2.4 商业秘密权益初步确权登记宜涵盖以下内容：

- 商业秘密权益登记名称；
- 商业秘密权益内容描述；
- 商业秘密载体存证记录；
- 商业秘密管理类载体存证记录；
- 登记日期。

8 商业秘密资产评估

8.1 评估原则

8.1.1 合法性原则：评估对象具备合法的形成过程、权属清晰，未侵犯第三方权益。

8.1.2 保密性原则：评估机构及参与人员与委托方签订保密协议，对商业秘密的内容、评估数据、评估报告等信息保密，避免泄露。

8.1.3 客观性原则：基于真实、准确的评估资料，采用科学的评估方法，独立开展评估工作，不受主观因素或外部干预影响。

8.1.4 价值匹配原则：结合商业秘密的保密期限、市场竞争力、产业化潜力等因素，评估结果与资产实际价值及应用场景相匹配。

8.2 评估方法

8.2.1 成本法：基于商业秘密资产的研发投入（如人力、物力、财力成本）、保密维护成本等，核算资产重置成本，结合资产损耗程度确定评估价值。

8.2.2 收益法：预测商业秘密资产在有效期内的预期收益（如销售收入增长、成本节约、许可费用等），采用合理的折现率将预期收益折算为现值，作为评估价值。

8.2.3 市场法：参考市场上同类商业秘密资产的转让、许可案例价格，结合资产自身特性（如技术先进性、市场独占性等）进行调整，确定评估价值。

9 商业秘密资产运营方式

9.1 联合研发

9.1.1 合作前准备

9.1.1.1 对联合研发伙伴进行商业秘密保护能力评估，包括保密制度建设、技术防护措施、过往保密履约情况等。

9.1.1.2 与联合研发伙伴签订联合研发保密协议，明确双方的保密义务，包括涉密信息的范围、保密期限、泄密责任等；同时签订研发成果归属协议，明确联合研发产生的商业秘密归属和利益分配。

9.1.1.3 划定联合研发中的涉密信息披露范围，根据研发分工和需求，仅向联合研发伙伴披露必要的商业秘密信息，核心密点可采取技术隔离或分阶段披露的方式。

9.1.1.4 可对联合研发过程中需要披露的商业秘密进行商业秘密权益初步确权登记。

9.1.2 研发过程管理

9.1.2.1 建立联合研发项目保密管理机制，明确双方项目组成员的保密责任，对参与研发的人员进行保密培训，签订个人保密承诺。

9.1.2.2 研发过程中产生的涉密文档、数据等实行统一管理，采用加密存储和传输，设置访问权限，对操作进行全程日志记录。

9.1.2.3 定期召开保密会议，通报项目保密情况，排查泄密风险，及时解决保密管理中出现的问题。

9.1.3 研发成果保护

9.1.3.1 对研发成果的载体进行固化和存证，包括技术文档、实验数据、样品等，建立成果档案，采取加密存储、专人保管等保护措施。

9.1.3.2 及时识别研发成果中的商业秘密并通过商业秘密权益初步确权登记明确保护范围。

9.1.3.3 监督合作方履行保密协议，定期核查其保密情况，发现违规行为及时采取维权措施。

9.2 委外生产

9.2.1 合作方筛选与协议签订

9.2.1.1 对委外生产厂商进行保密审核，重点评估其生产场地的保密设施、人员保密管理、生产流程中的保密措施等，选择具备相应保密能力的厂商。

9.2.1.2 可对生产标的涉及的商业秘密进行商业秘密权益初步确权登记。

9.2.1.3 与委外生产厂商签订保密协议，明确涉密信息（如产品配方、生产工艺、技术参数等）的披露范围、保密要求以及泄密后的赔偿责任等。保密协议宜约定委外生产过程中产生的边角料、报废品等涉密载体的回收和销毁方式。

9.2.2 生产过程保密管理

9.2.2.1 向委外生产厂商披露涉密信息时，采取分级披露、分段交付的方式，避免一次性披露全部核心技术信息。

9.2.2.2 对委外生产厂商的生产场地进行保密监督，引导其划定涉密生产区域，采取物理隔离、视频监控等保护措施。

9.2.2.3 定期对委外生产过程进行保密检查，核查涉密信息的使用情况、涉密载体的管理情况，发现泄密隐患及时要求整改。

9.2.3 后期管理

9.2.3.1 生产完成后，敦促委外生产厂商及时归还全部涉密文档、数据载体，回收剩余的涉密原材料、边角料、报废品等，进行统一销毁并保留销毁记录。

9.2.3.2 可对委外生产厂商的保密义务履行情况进行评估，形成评估报告，作为后续合作的重要依据。

9.2.3.3 持续监督委外生产厂商在保密期限内的保密行为，防止其在合作结束后泄露商业秘密。

9.3 交易许可

9.3.1 许可前评估与协议签订

9.3.1.1 对拟进行许可的商业秘密资产进行商业秘密权益初步确权登记，明确许可的内容及范围。

9.3.1.2 对商业秘密资产进行价值评估，确定合理的许可费用和许可方式。

9.3.1.3 对被许可方进行资质审核，评估其商业秘密保护能力和履约能力，避免向不具备保密条件或信誉不佳的主体许可。

9.3.1.4 签订商业秘密许可合同，明确许可的期限、使用方式、许可费用及支付方式等，同时约定保密义务，包括被许可方对商业秘密的保护措施、使用限制、不得向第三方披露等；明确违约责任，包括违约金、损失赔偿等。

9.3.2 许可过程管理

9.3.2.1 向被许可方交付商业秘密载体时，采取保密措施并提供必要的指导，避免披露超出许可范围的信息。

9.3.2.2 定期对被许可方的保密情况进行检查，核查其是否存在超范围使用、泄露商业秘密等违规行为，发现问题及时制止并追究责任。

9.3.3 许可后续管理

9.3.3.1 许可期限届满后，被许可方停止使用商业秘密，归还全部涉密载体，销毁自行复制的涉密资料。

9.3.3.2 对商业秘密资产的保密状态进行评估，若仍具有保密价值，继续采取相应的保护措施；若因许可使用导致部分信息公开，及时调整保护策略。

9.4 作价入股

9.4.1 入股前准备

9.4.1.1 委托具备资质的专业评估机构对商业秘密资产进行价值评估，出具合法有效的评估报告。

9.4.1.2 评估对入股对象的经营状况、财务状况、商业秘密保护能力、发展前景等，确保入股后商业秘密资产的安全和价值实现。

9.4.1.3 签订商业秘密作价入股协议，明确商业秘密的价值、入股比例、权利归属、使用限制、保密义务、利益分配等核心条款。

9.4.2 入股后管理

9.4.2.1 向目标公司移交商业秘密资产时，明确移交的范围和方式，采取加密移交、分阶段披露等措施，确保核心密点的安全。

9.4.2.2 积极参与目标公司的商业秘密管理，推动目标公司建立完善的商业秘密保护制度，包括人员管理、信息保护、涉密区域管理等，监督保密措施的落实。

9.4.2.3 对商业秘密资产的使用情况进行监督，确保目标公司仅在约定的范围内使用，不得超范围使用或向第三方披露。

9.5 质押融资

9.5.1 选择具备商业秘密质押融资业务资质的金融机构，签订质押合同和保密协议，明确质押标的、质押期限、借款金额、利率、还款方式，以及金融机构的保密义务、质押期间商业秘密的使用限制等。

9.5.2 可通过商业秘密权益初步确权登记明确质押融资的标的。

9.5.3 办理质押融资期间，加强对商业秘密资产的保护，避免在办理质押融资的过程中泄密。

9.6 保险

9.6.1 根据商业秘密资产的价值和面临的泄密风险，选择合适的商业秘密保险产品，明确保险责任范围、保险金额、保险期限、免赔额、理赔程序等。

9.6.2 向保险公司如实披露商业秘密资产的相关信息，包括价值、风险等。

9.6.3 可向保险公司提供商业秘密权益确权登记以及商业秘密合规管理登记证书作为申请参保的材料。

9.6.4 保险期间内，持续完善商业秘密保护措施；发生泄密事故时，及时通知保险公司，配合其进行损失核定和理赔工作。

10 商业秘密资产运营保护

10.1 保护原则

10.1.1 全流程保护：贯穿商业秘密资产运营的全环节（如联合开发、委托生产、技术出海、质押融资等），实现事前预防、事中控制、事后追责的闭环管理。

10.1.2 分级保护：根据商业秘密资产的重要程度（如核心级、重要级、一般级），采取差异化的保护措施，重点保障核心商业秘密的安全。

10.1.3 权责明确：明确企业内部各部门、各岗位及合作方的保密责任，建立“谁运营、谁负责，谁接触、谁保密”的责任机制。

10.1.4 动态适配：结合运营场景的变化及时优化保护措施，应对新的保密风险。

10.2 保护措施

10.2.1 制度保护措施包括但不限于：

- 建立商业秘密运营保密管理制度，明确保密范围、保密职责、泄密处置流程等；
- 制定针对不同运营场景的专项保密操作规范，指导相关人员执行。

10.2.2 人员保护措施包括但不限于：

- 对参与商业秘密运营的内部人员进行保密培训，考核合格后方可上岗；
- 在劳动合同中约定保密条款；
- 与核心涉密人员签署竞业限制协议；
- 对可能接触到商业秘密的外部人员进行保密告知并签署保密协议。

10.2.3 技术保护措施包括但不限于：

- 采用加密技术（如文件加密、传输加密、存储加密）、访问控制技术（如分级授权、指纹/人脸认证）、数据脱敏技术、水印技术等，防止商业秘密信息被非法获取、复制、传播；
- 安装泄密监测系统，实时监控信息流转状态，及时发现异常访问或泄露行为。

10.2.4 物理保护措施包括但不限于：

- 对存储商业秘密资产的场所（如办公室、数据库机房）采取门禁管理、视频监控、防盗设施等物理防护措施；
- 对承载商业秘密的载体（如电脑、U 盘、纸质文件）进行统一管理，标注保密标识，明确保管责任。

10.3 泄密应急处置

10.3.1 建立泄密应急预案，明确应急组织机构、响应流程及责任分工。发现泄密事件后，立即启动应急预案，控制泄密范围扩大（如撤回泄露信息、终止违规访问权限等）。

10.3.2 及时收集泄密相关证据（如访问日志、传输记录、沟通记录等），查明泄密原因、泄密范围及责任人，必要时委托专业机构进行司法鉴定。

10.3.3 对内部泄密责任人，依据保密管理制度及劳动合同进行处分；对外部合作方或第三方泄密者，根据保密协议约定追究违约责任，或通过民事诉讼、行政投诉、刑事报案等方式维护权益。

10.3.4 针对泄密事件暴露的问题，完善保密管理制度与保护措施，加强人员培训与风险排查，避免同类事件再次发生。