深圳市人民检察院

商业秘密刑事保护体系合规建设指引

(试行)

前言

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。技术信息是指权利人采取了保密措施不为公众所知悉的，具有经济价值的技术知识信息，包括制造技术、设计方法、生产方案、产品配方、研究手段、工艺流程、技术规范、操作技巧、测试方法、技术诀窍等技术信息。经营信息是指技术信息以外，经权利人采取了保密措施不为公众所知悉的，具有经济价值，能给权利人带来竞争优势的用于经营的信息，包括战略规划、管理方法、商业模式、销售渠道、客户信息、原材料价格、产销策略、财务信息、资源储备、招投标事项等经营信息。

商业秘密是企业的无形资产，是企业核心竞争力的重要体现。商业秘密的有效保护能使企业在激烈的市场竞争中持续保持优势，有利于激发企业创新活力，增强企业内生动力，推动企业实现高质量发展。

商业秘密保护关系企业安全。在企业发展初期，专利申请、维护以及信息披露的成本较高，依靠商业秘密保护为主、专利保护为辅的知识产权保护策略，能够在实现核心技术保护的同时，兼顾运营自由与成本管控。在企业存续期间，商业秘密保护是企业安全的重要保障，是企业持续生存和发展的关键，对于重要商业信息的严格保密，有利于企业在实现信息“垄断”的同时，移固市场地位。

商业秘密凝聚了企业在社会经济活动中创造的智力成果，而一旦商业秘密被侵犯，对企业造成的伤害不可估量。在选择侵权救济途径时，除民事起诉或提起行政程序外，越来越多企业考虑通过刑事控告的手段进行救济。但从目前一些案件来看，多数企业对于商业秘密的保护意识不强、行动不够，在商业秘密生成后未能采取有效管控措施，在商业秘密被侵犯后未能采取有效维权措施，与刑事保护体系的基本要求严重不符，客观上也造成了商业秘密刑事维权难的现象。此外，在当前企业人员流动、商业技术合作、跨境经营交往等日益增多的背景下，企业在商业秘密合规风险防范工作方面的不足，也可能导致被动陷入商业秘密侵权纠纷。

本指引旨在帮助企业加强商业秘密刑事保护，管控商业秘密合规风险，更好维护企业合法权益与公平竞争的市场秩序。指引依据有关法律、法规等规范性文件，结合刑事司法实践与企业商业秘密保护与管理实际，在具体内容上包括了商业秘密确定、涉密人员管理、保密措施管理、保密信息管理、商业秘密外部管理、商业秘密侵权维权、合规风险防范等七部分内容，涵盖商业秘密刑事保护及合规工作的方方面面及其中的重难点问

题，能够为企业开展商业秘密刑事保护体系合规建设工作提供清晰有效的指引。

指引Ⅰ：商业秘密确定

商业秘密确定是商业秘密刑事保护体系合规建设的源头性和基础性工作，在企业确定通过商业秘密手段保护商业信息时，首先要做的是在内部识别具体需要保密的商业信息，确定并及时更新保密清单，明确清单内各项商业秘密的权利归属、保密级别、保密期限以及知悉范围等，以为企业商业秘密刑事保护体系合规建设工作提供基本支撑。

1.商业秘密识别

企业应根据发展阶段、竞争优势、所处行业特性、相关产品特点以及商业秘密相关法律法规等，结合自身实际确定商业信息保护方式。对于需要通过商业秘密手段进行保护的商业信息，企业应及时将其识别为商业秘密，列入保密清单，进行保密管理。

推荐重点工作清单：

1.1 研判相对于专利保护，采取商业秘密手段对技术信息进行保护，是否有利于降本增效等；

1.2 研判相对于专利保护，采取商业秘密手段对技术信息进行保护，是否有利于实现技术独占、技术成果保密以及进一步研发；

1.3 根据产品技术结构、控制过程、制作工艺等是否容易被反向工程，确定是否采取商业秘密手段对技术信息进行保护；

1.4 研判相关行业壁垒是否较高，是否不宜采用申请专利等信息公开策略等对商业信息进行保护；

1.5 评估商业信息的价值，包括获取该商业信息的难度、能够增加的竞争优势、商业信息泄露造成的损害以及能够实现或者是潜在能够实现的经济价值等；

1.6 评估采取商业秘密手段对商业信息进行保护，是否有利于稳固市场地位、增强营销效果；

1.7 评估其他相关因素，考量商业信息是否适宜通过商业秘密手段进行保护。

2.商业秘密权属

企业应与员工、管理人员、股东、合作伙伴等明确约定商业秘密的权利归属，包括所有权、使用权、转让与许可权、收益权以及商业秘密成果

归个人时的优先使用权等。

推荐重点工作清单：

2.1 与研发人员签订书面协议，明确约定在职期间完成本职工作或主要利用本企业的物质技术条件所产生的商业秘密的权利归属；

2.2 与以商业秘密作为技术入股的股东、管理人员、员工等签署商业秘密入股协议，并对商业秘密权利归属进行约定，明确相关人员在职期间商业秘密的权利归属；

2.3 与合作伙伴签署技术开发合同，技术开发合同应当包括商业秘密权利归属条款，明确约定共同合作产生的商业秘密的权利归属；

2.4 对于员工在职务范围之外研发的商业秘密，企业如想要获得相关权利，应与研发员工签订协议，明确约定商业秘密的权利归属。

3.商业秘密定级

企业应遵循充分保护、易于实施、降低成本等原则对商业秘密进行分级管理。统一保护模式容易导致商业秘密保护过度或保护不足，而采取与商业秘密对应的适当保密措施则更有利于提高保密效率。

推荐重点工作清单：

3.1 根据商业秘密的数量、重要程度、经济价值、保护要求、管理水平等实际情况划分商业秘密的密级：

3.2 具体可考虑将商业秘密分为核心商业秘密、重要商业秘密以及一般商业秘密三级或核心商业秘密、一般商业秘密两级；

3.3 密级变更一般由业务部门提出，经企业相关负责人审批后确定。

4.商业秘密保密期限

企业应根据商业秘密的密级、生命周期、潜在价值、市场需求、保密成本以及相关行业竞争现状等因素，确定商业秘密的保密周期。

推荐重点工作清单：

4.1 可以预见时限的以年、月、日计算，难以预见时限的应定为“长期”或者“公布前”；

4.2 对于预见不足，需延长或缩短商业秘密保密期限的，应及时对商业秘密保密期限进行调整；

4.3 保密期限调整一般由业务部门提出，经企业相关负责人审批后确定新的保密期限。

5.商业秘密知悉范围

企业应根据工作需要严格确定商业秘密的知悉范围，避免因知悉范围过大给商业秘密的管控带来难度。

推荐重点工作清单：

5.1 应将知悉范围明确限定到具体的岗位和人员，并按照涉密程度实行分级分管；

5.2 不得允许与履行职责无关的人员以及第三方随意接触商业秘密；

5.3 对于因工作需要、推广应用等原因需扩大商业秘密知悉范围的，应严格履行审批手续，在获得批准前，严禁无关人员接触商业秘密。

指引Ⅱ：涉密人员管理

涉密人员是“生产”、使用和管理企业商业秘密的主体，涉密人员管理质量的高低直接关系企业商业秘密保护工作的成败，是企业商业秘密刑事保护体系建设的关键。实践来看，企业商业秘密保护工作出现问题，绝大多数可归结为人的问题，企业一旦放松涉密人员管理，就可能导致商业秘密的泄露，给企业生产经营造成损害。因此，企业商业秘密刑事保护体系及合规建设工作必须将涉密人员管理摆在前列，严格利用制度约束，将保密责任与义务落实到涉密人员的具体工作中去。

6.人员入职管理

企业应注重人员入职管理，对新入职人员进行商业秘密风险识别与防控。

推荐重点工作清单：

6.1 注重人员招聘管理，避免在沟通交流、招聘笔试、招聘面试等环节不当获取他人或泄露公司的商业秘密；

6.2 与新员工签署保密协议，约定保密范围、保密期限、双方权利义务以及违约责任等内容；

6.3 对于新入职的高级管理人员、高级技术人员以及其他知悉核心、重要商业秘密的人员，企业还应与其签署竞业限制协议，约定竞业限制的范围、地域、生效条件、期限、违约责任以及经济补偿等，竞业限制协议不得违反相关法律法规；

6.4 及时安排入职保密培训，未经保密培训不得上岗，保密培训内容应当包括相关法律法规培训、企业保密制度培训、岗位保密职责培训等，确保员工理解企业商业秘密管理的制度及程序，树立保密意识，理解保密

责任。

7.人员日常管理

企业应遵循“先岗后人”“人随岗定”“精确限定”等原则，对企业涉密人员进行日常管理，即先确定涉密岗位，在涉密岗位上工作的人员应被确定为涉密人员。

推荐重点工作清单：

7.1 形成涉密岗位及涉密人员清单，并根据岗位变动及人员流动情况及时更新；

7.2 做好日常保密培训，确保员工特别是涉密岗位员工熟知在职期间的权利和义务，明确相关商业秘密的保密方法与操作规则，了解泄露企业商业秘密可能带来的法律风险，知悉泄露企业商业秘密需要承担的违约责任等，通过日常培训，不断强化企业员工的保密意识，提高员工的保密能力；

7.3 对于临时性、阶段性重要专项工作，企业应结合实际确定涉密岗位和涉密人员，对涉密岗位工作人员进行全面审查，做好成果保密工作，确保专项工作安全运转；

7.4 定期开展商业秘密保密自查巡查，要求涉密人员签署保密承诺书，对涉密人员进行监督检查，对涉密人员履行保密职责情况考察审核；

7.5 对于在保密自查巡查中发现的异常情况，如发现商业秘密泄密或造成重大泄密隐患等情况，应及时上报、快速处置；

7.6 做好保密交接工作，要求涉密员工在工作调动时规范交接，前任、后任工作人员对各类涉密设备、信息载体、文件资料等逐一清点、登记，形成交接台账。

8.人员离职管理

涉密人员是企业的“顶梁柱”，一旦涉密人员带着商业秘密跳槽到竞争企业，可能会给企业造成重大损失，制定相应的保密制度以及做好离职员工的管理也是商业秘密刑事体系合规建设的重要内容。

推荐重点工作清单：

8.1 通过技术等手段提前对离职人员工作电脑的一些异常操作、关键词识别、邮箱文件的处理、文件传输以及文件打印等进行监控，以获取异常操作点或异常行为反馈，但需注意不能窃取员工的个人隐私信息；

8.2 进行离职面谈,告知员工保密义务不因劳动合同的解除，终止而免除，其他约定注意事项亦应在离职后遵守；

8.3 对离职人员的电脑等涉密设备进行清查，对信息载体、文件资料

及其他相关物品进行盘点，对信息系统权限进行回收，督促员工交接涉密信息资料，返还或者按照要求销毁涉密载体等；

8.4 对于涉密人员，企业应评估是否需要履行与离职员工签署的竞业限制协议或者重新签订竞业限制协议，竞业限制协议的约定不得违反相关法律法规；

8.5 应定期追踪人员离职后的去向，重点关注员工离职后到与本企业有竞争关系的企业任职，或者自己创业生产或者经营与原企业同类产品、从事同类业务的情况，及时发现涉密信息泄露或者不当使用的线索。

指引Ⅲ:保密措施管理

采取保密措施是相关商业信息能够作为商业秘密受到法律保护的必要条件，有关商业秘密保护的法律法规并未要求保密措施可以对商业秘密的保护严丝合缝、万无一失，但这绝不意味着相关法律法规对商业秘密保密措施没有任何要求，企业断不可通过宽泛的、流于形式的保密措施对商业秘密实施保护。一般来说，企业所采取的保密措施应在同行业中被认为是基本合理的，达到在正常情况下足以防止商业秘密泄露的标准。

9.涉密专区管理

企业应按照涉密信息生成场所以及涉密载体存放场所等在企业内部划分商业秘密保护专区，并采取相适应的措施对专区进行保密管理。其中涉密信息生成场所主要包括涉密产品研发场所、涉密产品生产场所等;涉密载体存放场所主要包括涉密信息存储中心、涉密档案室、涉密产品存放场所等。

推荐重点工作清单:

9.1 根据具体涉密信息加强涉密专区管理，一般应对涉密信息生成场所以及涉密载体存放场所等采用门、墙、隔断等物理措施进行防护隔离，形成“独立封闭”的专门区域；

9.2 对涉密人员进入专区可实行登记或刷卡管理等方式进行实时记录；

9.3 对非涉密人员进入专区进行严格审批、登记，同时应由企业专门人员等全程陪同进入专区，严防商业秘密泄露；

9.4 在涉密专区显著位置张贴非请勿入、禁止拍摄、禁止携带违禁品等禁止性警示标识，对于特定涉密专区，建议企业采取禁止携带手机、相机等具有拍摄功能的电子设备进入等方式加强涉密专区管理；

9.5 在涉密专区范围内安装视频监控、报警装置等安防设备，在涉密专区出入口配备安保人员或安装视频监控、报警装置等安防设备。

10.涉密设备管理

涉密设备一般指采集、存储、处理、传输涉及企业商业秘密的计算机设备、通信设备、复印件、传真机、碎纸机等设备。

推荐重点工作清单：

10.1 企业涉密设备应登记造册，由专人负责，实行标签化管理；

10.2 涉密设备的领取、使用、流转、维修、报废等一律应履行审批、登记等手续，严控涉密设备的“使用”；

10.3 对于具备信息存储功能的涉密计算机设备等，应使用云桌面系统进行办公，统一存储涉密信息，避免将涉密信息分散存储于涉密设备的本地存储中；

10.4 对涉密设备用户登录权限、账户、密码等实行统一授权、管理；

10.5 建立涉密用户操作日志，实时记录并定期检查用户登陆、获取信息和异常侵入等情况；

10.6 对于异常侵入等不正常情况，应及时追查，发现确有问题的，应及时处置，避免商业秘密泄露；

10.7 企业应在涉密设备显著位置或是涉密设备电子操作界面进行保密提醒，明确标明保密设备的操作规则、注意事项以及涉密用户的保密责任与义务等。

11.涉密载体管理

涉密载体一般是指以数据、文字、符号、图片、视频、音频等方式记录商业秘密的各类纸张、胶卷、胶片、磁带、光盘、U 盘、硬盘等有形存储载体。

推荐重点工作清单：

11.1 建立涉密载体管理制度，对涉密载体一般应标注保密标识，安排专人负责涉密载体管理；

11.2 对商业秘密载体的制作、收发、传递、保存、使用、维修、报废、销毁等实施全流程留痕管理，建立涉密载体管理台账，确保涉密载体安全；

11.3 对于涉密载体的使用施行严格审批与登记制度，严格依据涉密载体的使用权限，控制涉密载体的使用范围：

11.4 严格规范涉密载体处置，这里的处置主要包括维修、报废与销毁等，对于涉密载体的处置应履行审批与登记等手续，并将涉密载体交由专业、有资质的单位进行处置，同时应与相关处置单位签署涉密载体处置协

议，明确约定保密责任与义务。

12.信息系统管理

信息系统管理主要指企业对于涉密信息操作系统的管理，主要包括计算机信息系统、通讯信息系统以及办公自动化信息系统等软件操作系统及其配套网络信息系统等的管理。

推荐重点工作清单：

12.1 加强信息系统权限管理，确定责任部门统一管理涉密系统权限的授予，变更及回收等；

12.2 对信息系统的权限管理应保留记录日志，定期对照检查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；

12.3 在日常管理中严格区分并隔离涉密信息操作系统与非涉密信息操作系统，禁止以任何形式在两系统之间直接传输任何信息；

12.4 通过保密管理系统和杀毒软件等对涉密信息系统进行保密管理，避免或减少因违规外联、非授权登录、木马病毒以及恶意代码等漏洞与隐患可能造成的商业秘密泄露风险。

指引Ⅳ:保密信息管理

涉密信息资料直接关系企业生产经营安全和利益，必须妥善保管，以防泄漏。对于企业来说，必须坚持统一管理原则，建立保密信息存储、复制、流转、销毁等配套制度。对于企业管理人员和涉密人员来说，就是要强化保密信息管理意识，严格执行保密信息管理制度，坚决遵守保密信息管理规定，严防涉密信息管理“失位”。此外，企业保密信息管理还应强调各环节管理，通过申请--审批--执行等环节管理，避免保密信息处于监管“失控”状态。

13.信息存储管理

企业应指定专人负责商业秘密的存档和保管，并根据商业秘密的密级、载体情况、管理条件等确定合适的存管方式。

推荐重点工作清单：

13.1 使用保密柜等具有保密功能的设备存放涉密文件及载体；

13.2 在存放涉密载体的区域配备安保人员或安装视频监控、报警装置等安防设备；

13.3 对于载有涉密信息的电子文档可以采取添加加密等技术手段进行保密管理；

13.4 加强涉密信息存储台账管理，完善涉密信息储存、使用、处置等审批流程，尤其注重因人员变动带来的台账更新问题，确保商业秘密所涉信息存储存管可控等。

14.信息复制管理

企业应加强对于商业秘密信息的复制管理，企业员工未经授权不得复制涉密信息材料。

推荐重点工作清单：

14.1 因工作需要复制涉密信息材料的，应由相关责任人进行审批并保留记录；

14.2 企业员工采取纸质化等方式复制涉密信息材料的，应严格控制复制份数，并在复制时守候在复制设备旁，复制后应立即取走并妥善保管相关纸质复制材料；

14.3 对于因复制错误等原因需要销毁的涉密材料，应及时通过销毁程序进行销毁，不得随意处置。

15.信息流转管理

企业应加强商业秘密信息的流转管理，规范自身操作流程和管理机制，降低商业秘密流转过程中的泄露风险。

推荐重点工作清单：

15.1 涉密纸质文档的传递应采取密封包装、专人专车、保密快递等保密措施；

15.2 涉密电子文档应通过涉密网络进行传输，配备纸质或电子签收单，标明签收人和签收时间；

15.3 涉密物品等实物的流转，应采取包装、密封等保密指施；

15.4 商业秘密信息一般只能在企业内部流转，因工作需要流出到外部的需经严格审批。

16.信息销毁管理

商业秘密销毁是企业保护商业秘密的“最后一道关口”，对于保守企业秘密、维护企业利益具有十分重要的作用，企业应建立完善的商业秘密信息销毁制度。

推荐重点工作清单：

16.1 在销毁商业秘密信息、文件、资料、载体以及物品等前，应由相关业务部门提出，经企业相关负责人批准后实施；

16.2 企业可委托专业有资质的涉密信息处置单位销毁涉密信息，也可

自行销毁涉密信息；

16.3 对于自行销毁涉密信息的，企业应对涉密信息销毁进行全程监督，包括:要求相关人员签署涉密信息销毁保密协议，明确保密责任与义务;要求相关人员在企业视频监控范围内实施销毁;要求相关人员对销毁过程进行全程录像;要求不少于 2 名员工在销毁现场进行见证并在销毁凭证上签字。

指引Ⅴ:商业秘密外部管理

企业在信息发布、商业合作、技术合作、跨境合作以及并购重组等对外商业交往活动中，会不可避免地向客户或合作伙伴等透露企业的商业秘密，这是商业秘密外泄的一条重要渠道。企业在向外部人员和单位“提供”商业秘密信息前，应与其签订保密协议，明确相关外部人员和单位的保密责任与义务，其中保密协议原则上应在对外“提供”商业秘密信息前与相关直接接触商业秘密的外部人员和单位签署。

17.信息发布管理

企业因经营活动需要对外发布信息的，一般应由业务部门提出，企业相关负责人组织相关人员在信息对外发布前进行保密审查，符合对外发布条件的，可以批准对外发布。

推荐重点工作清单:

17.1 企业涉密人员因工作需要对外发表论文或讲座的，一般由涉密员工提出，企业相关负责人组织相关人员在信息对外发布前进行保密审查，符合对外发布条件的，可以批准对外发布;

17.2 企业在参加技术交流会、成果论证会、技术发展论坛等会议时应避免展示企业涉密技术资料，确有必要展示的，应将有关材料标注密级，指定已签署相关保密协议的与会人员接收并按要求返还;

17.3 企业应对广告宣传、成果展示等经营活动中对外发布的信息进行审查，避免涉密信息泄露，对于在成果展示中展出的涉密产品，企业可通过设立围挡、伪装覆盖、禁止拍照等方式保护企业商业秘密;

17.4 企业应定期追踪已对外发布的信息，对于追踪发现的异常情况，及时上报企业相关负责人排查处置，发现确有问题的。应及时采取补救措施。

18.商业合作保密

企业在开展投资合作、招投标合作等涉及经营信息合作以及涉及涉密

产品采购、销售等产品购销合作时，应重视商业秘密管理，避免在商业合作中造成商业秘密泄露。

推荐重点工作清单：

18.1 企业一般应避免将商业秘密向商业合作伙伴公开；

18.2 采用签订保密协议等方式约定商业合作伙伴在合作洽谈期间、合作期间及合作后对其掌握、了解的相关商业秘密的保密责任与义务，以降低商业秘密在商业合作中被泄露的风险；

18.3 在商业合作期间以及合作后应定期对保密协议履行等情况进行监督，对于监督发现的异常情况，及时上报企业相关负责人排查处置，发现确有问题的，应及时采取补救措施。

19.技术合作保密

企业应加强对合作研发、委托研发、授权许可、转让出售等技术合作中对千商业秘密的保密管理。

推荐重点工作清单：

19.1 在开展技术合作时，应充分调查合作方的商业秘密管理能力及侵权风险，并与合作对象签订保密协议等，约定商业秘密的使用权限、日常管理以及争议处理等内容：

19.2 涉及研发合作的，需明确约定共同开发、委托研发、改进或二次研发中涉及的“新”商业秘密的权利归属，包括所有权、使用权、转让与许可权、收益权以及商业秘密成果归员工个人时的优先使用权等，并明确各方权利义务等内容；

19.3 在技术合作期间以及合作后应定期对保密协议的履行等情况进行监督，对于监督发现的异常情况，及时上报企业相关负责人排查处置，发现确有问题的，应及时采取补救措施：

19.4 在聘任或者委托专家、顾问、翻译等专业人员合作“处理”企业商业秘密时，应对专业人员的背景进行调查，了解其保密能力、侵权风险以及此前合作企业等情况，避免选择与竞争企业有业务往来的专业人员；

19.5 在技术合作中，企业应与外部专业人员签订保密协议，明确约定保密责任与义务。

20.跨境合作保密

企业在进行跨境合作时，要特别注重商业秘密保护，完善跨境合作安排，为高效开展跨境合作提供安全保障。

推荐重点工作清单：

20.1 聘请专业人员考察了解境外合作伙伴的商业秘密管理能力、商业秘密侵权风险等;

20.2 通过签订保密协议等方式约定商业秘密的使用权限，日常管理以及争议处置等内容;

20.3 涉及跨境研发合作的，还需明确约定共同开发、委托研发、改进或者二次研发中涉及的“新”商业秘密的权利归属，句括所有权、使用权、转让与许可权、收益权以及商业秘密成果归员工个人时的优先使用权等，并明确各方权利义务等内容;

20.4 在跨境合作期间以及合作后应定期自行或聘请专业人员对保密协议的履行情况进行监督，对于监督发现的异常情况，及时上报企业相关负责人排查处置，发现确有问题的，应及时采取补救措施。

21.并购重组保密

企业在并购重组过程中应采取有效措施降低商业秘密泄露风险，其中被收购企业在并购交易中尤其要重视商业秘密的泄露风险。

推荐重点工作清单:

21.1 在收购企业对被收购企业开展尽职调查之前，被收购企业应要求与收购企业以及收购企业的中介机构签订保密协议或是由收购企业出具保守企业商业秘密的保密函，明确禁止收购企业及中介机构将获悉的商业秘密外传;

21.2 被收购企业对尽职调查所提供的涉密文件及材料等一般应制作交接台账，由收购企业或中介机构签收确认;

21.3 若在尽职调查后未达成收购协议，一般应按照交接目录收回已提供的涉密文件及材料的原件及复制件;

21.4 在并购重组中，涉及被收购企业核心商业秘密的，被收购企业应当审慎决定是否提供给收购企业或是中介机构，其中确有必要提供核心商业秘密的，可允许收购企业现场查阅，一般不得拍照、复印和摘录。

指引Ⅵ:商业秘密侵权维权

从实践来看，企业商业秘密维权总有绕不过的“坎”诸如举证难、赔偿低、周期长、成本高、效果差等声音不绝于耳。这种情况一方面是由商业秘密案件的复杂性、专业性以及商业秘密侵权的多样性、隐蔽性等特点造成，另一方面也是因为企业未能采取合理有效的侵权维权措施等原因导致。因此，解决商业秘密维权难的问题，企业必须先从自身开始重视商业秘密侵权维权，在发现商业秘密被侵权时，迅速启动应急预案、收集侵权

证据、评估侵权行为等，并根据侵权行为评估结果，及时确定维权途径。快速进行侵权维权，避免侵权损失的扩大。

22.应急预案生效

企业应制定商业秘密泄露或者被侵权的应急处置预案，包括发现、制止、处置、取证、追责等应急处置流程。

推荐重点工作清单：

22.1 强化日常监管等及时发现商业秘密泄露等情况，在发现商业秘密泄露后，应急预案立即生效；

22.2 企业发现商业秘密泄露应立即制止，包括制止物理搬运、超量下载、异常登录等；

22.3 企业在制止商业秘密泄露后，应立即采取补救措施防止损失扩大，包括物理措施、技术措施、法律措施以及制度措施等；

22.4 企业在发现商业秘密泄露并采取手段及时制止与补救后，应立即开展取证工作，为下一步追责问责、改善管理等做好准备；

22.5 追究责任的实质主要是指追究法律责任，包括民事责任、行政责任和刑事责任。

23.侵权证据收集

企业发现商业秘密被侵权后，应及时会同专业法务或律师一并收集、固定证据。

推荐重点工作清单：

23.1 对容易丢失的证据及时公证，对取证现场进行视频拍照，对重要人员进行访谈做笔录等；

23.2 对于超出企业取证能力的证据收集与获取，应及时请市场监管部门、公安机关等相关部门介入；

23.3 收集、固定关于商业秘密享有权利的证据，包括体现商业秘密的载体、电子数据、存证证明等；

23.4 收集、固定关于商业秘密不为公众所知悉的证据，必要时可委托鉴定机构出具非公知性鉴定报告；

23.5 收集、固定关于商业秘密采取保密措施的证据，包括保密制度、保密措施、保密管理等；

23.6 收集、固定关于商业秘密具有经济价值的证据，包括商业秘密的现实价值与潜在价值，必要时可委托评估机构进行价值评估；

23.7 收集、固定关于泄密人员相关信息的证据，包括个人基本信息、工作岗位信息、财产相关信息等；

23.8 收集、固定关于商业秘密被侵犯的证据，包括被窃取、披露、使用等证据，必要时可委托鉴定机构进行鉴定；

23.9 收集、固定企业因被侵权造成的销售利润的损失、商业秘密的合理许可使用费、商业秘密的研发成本、实施该项商业秘密的综合收益、侵权获得的财物或财产性收益等证据；

23.10 收集、固定企业为减轻对商业运营、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的证据；

23.11 收集、固定企业为维权所支付的合理开支费用等证据，

24.侵权行为评估

企业在发现商业秘密侵权线索后，应在开展侵权证据收集的同时对侵权行为进行评估，确定受损程度及合适的补救措施。

推荐重点工作清单：

24.1 立即展开内部调查，确定商业秘密是否受到侵犯以及受侵犯的程度，评估可以采取的合适的补救措施；

24.2 在商业秘密侵权风险发生后，应及时分析风险发生原因，评估企业现行商业秘密管理制度、技术方案及落实情况等存在的漏洞与不足；

24.3 根据侵权行为评估结果对照完善相关保密工作流程，防止商业秘密侵权风险再次发生。

25.维权途径确定

刑事控告是商业秘密侵权最严厉的打击措施，也是证据标准最严格的维权途径，在某些情况下，因数额、证据等原因不足以支持刑事控告，对此企业可根据实际情况，灵活确定维权途径。

推荐重点工作清单：

25.1 根据侵权行为评估的结果，确定商业秘密侵权维权的途径和方案；

25.2 关于商业秘密侵权，企业可选择的维权途径一般包括：协商解决；请求调解组织调解；向市场监督管理部门投诉；涉及劳动关系的可向劳动仲裁机构申请仲裁；根据仲裁条款或仲裁协议提请仲裁机构仲裁：向人民法院提起民事诉讼：向公安机关控告；向人民法院提起刑事自诉；申请人民检察院对商业秘密诉讼活动进行监督等。

指引Ⅶ：合规风险防范

商业秘密是企业保持竞争优势的无形财产，企业应当树立正确的经营观念，认真学习和了解商业秘密有关法律法规，通过加大研发及商业投入等培育自身具备竞争优势的商业秘密，避免通过不正当手段获取商业秘密的方式为企业谋求发展。此外，企业在日常经营中不仅应强调刑事保护体系建设，亦应重视合规风险防范工作。这里的合规风险防范主要指的是在事前主动构建商业秘密合规管理体系，达到防止侵犯他人商业秘密的目的，避免因人员管理疏忽、合作风险不明、研发存档不善以及域外法律风险不查等原因陷入本可避免的商业秘密侵权纠纷。

26.入职人员背调

对于入职人员，企业需要重点防范其“引入商业秘密侵权的风险”，即调查核实其有无从第三方带来他人的商业秘密等情况。

推荐重点工作清单：

26.1 企业在进行人员招聘以及吸纳技术人员以商业秘密入股企业时，应重点核实待入职人员是否违反与前任雇主的保密义务、竞业限制协议或者发生其他侵犯及损害前任雇主商业秘密的情形；

26.2 对于有涉密岗位工作背景或存在一定商业秘密侵权风险的人员，企业还需对其相关背景信息进行第三方背调或尽调，如排查该人员相关研究领域的技术文献、检索相关专利申请等；

26.3 企业一般还应与入职人员签署不侵犯前任雇主商业秘密等知识产权承诺书。

27.秘密权属查明

除自行“研发”外，企业还可能通过员工入职、技术入股、技术合作、并购重组等途径获得商业秘密，这些商业秘密“由外入内”，其本身可能存在的风险相对较高，企业应重视其权利归属的查明，避免因权属不清可能给企业带来的法律及经济风险。

推荐重点工作清单：

27.1 重视通过外部途径获取商业秘密权利归属的查明，包括查明商业秘密的所有权、使用权、转让与许可权、收益权等；

27.2 与商业秘密“提供方”签署承诺书，要求承诺权属完整性以及不侵犯任何第三方商业秘密等。

28.合作风险防范

企业在进行商业合作、技术合作、跨境合作等商业活动中应重视对于合作方背景的调查，包括合作方商业秘密管理能力、合作方商业秘密合规

风险等，避免因合作管理不当给企业带来的法律风险及经济损失。

推荐重点工作清单：

28.1 涉及技术合作的，应对技术合作所涉商业秘密进行尽职调查，如排查相关研究领域的技术文献、检索相关专利申请等；

28.2 对合作事项进行综合评估，评估内容包括合作方的经营管理能力、合作所能产生的经济价值、合作可能存在的法律风险等；

28.3 必要时可要求合作方签署承诺书，承诺双方合作不侵犯任何第三方商业秘密等；

28.4 对于在合作洽谈期间、合作期间及合作后接收到的对方保密信息，应注重风险防范,对照合作保密要求做好保密工作，避免因泄露对方保密信息而造成的不必要法律纠纷。

29.研发记录存档

企业在商业秘密生成过程中，应注重研发记录的存档、使用。一是能够在一定程度上确保企业而不是“个人”掌握商业秘密，另一方面在于存档的原始研发记录能够作为对外主张权利的依据。

推荐重点工作清单：

29.1 对于项目立项书、研发测试数据、产品实验数据等原始研发文档的实时或定期记录与存档；

29.2 应对原始研发文档采取与商业秘密同等的保密措施，避免因原始研发文档的泄露造成商业秘密本身的泄露；

29.3 在企业或相关人员被主张涉嫌商业秘密侵权时，可通过提供自主研发记录等主张商业秘密是企业自主研发来进行侵权抗辩。

30.国际业务评估

企业在投资、经营以及合作等商业活动中涉及到国际业务的，应对国际业务所涉商业秘密法律风险进行充分评估，并根据评估结果调整企业商业秘密合规管理机制。

推荐重点工作清单：

30.1 在开展国际业务前应深入研究当地相关法律法规及有关商业秘密禁止性规定等文件，必要时可委托有相关资质的专业第三方机构出具评估报告；

30.2 在开展国际业务时应对照事前评估报告，严格遵守当地有关商业秘密法律法规及规范性文件，避免因违反有关禁止性规定给企业造成的损害；

30.3 在当地开展国际业务合作时，应对当地合作方背景进行调查，对

合作可能带来的商业秘密合规风险作出提前预判，避免因合作方的问题导致法律纠纷。

《商业秘密刑事保护体系合规建设指引（试行）》发布解读

一、《指引》的制定过程

商业秘密作为企业的无形资产，是企业的核心竞争力。商业秘密被侵犯或陷入商业秘密纠纷，将直接导致企业竞争优势丧失、市场占有率下降，严重影响企业发展，极端情况下甚至导致企业生存危机。商业秘密保护对企业，特别是高新科技企业的发展安全至关重要。越来越多的企业在选择商业秘密侵权救济途径时，考虑刑事控告。但从目前一些侵犯商业秘密刑事案件来看，多数企业，特别是初创期和快速成长期的中小型高新科技企业，对商业秘密的保护意识不强、行动不够，在商业秘密生成后未能采取有效管控措施，在商业秘密被侵犯后未能采取有效维权措施，客观上造成了商业秘密刑事维权难的现象。部分企业在人员聘用和商业交往中对他人商业秘密保护关注不够，容易陷入商业秘密纠纷，影响企业发展。

为进一步加强商业秘密保护，激发社会创新创造活力，帮助企业构建与刑事保护基本要求相匹配的商业秘密管理体系，深圳市检察院知识产权检察办公室专门组织开展课题研究，从2022年4月开始，对近年来深圳市商业秘密刑事案件开展全面梳理总结、分析研究，并与市场监管、公安等相关职能单位深入交流，用时一年，于2023年2月，起草完成《指引》，向企业、律所等市场主体广泛征求意见，收到包括华为、苹果、腾讯、大疆、顺丰、荣耀、OPPO、安世半导体、拓邦、思摩尔等知识产权优势企业和方达所等顶级红圈律师事务所的积极反馈意见，现《指引》已根据反馈意见修改完善，正式发布。

二、《指引》的主要内容

《指引》由前言和正文组成，前言部分简单介绍了背景和目的。正文对商业秘密刑事保护体系合规建设给出了7大类，30大项，125小项的指引。具体包括：

（一）商业秘密确定。《指引》从商业秘密识别、商业秘密清单确定及更新、商业秘密权利归属、保密级别、保密期限、知悉范围等关键要素给出了5大项20小项指引，为企业商业秘密刑事保护体系合规建设提供基本支撑。

（二）涉密人员管理。《指引》从入职管理、日常管理、离职管理等方面给出了3大项15小项指引，引导企业确保对涉密人员“全流程”管理，将保密责任与义务落实到涉密人员具体工作中。

（三）保密措施管理。《指引》从涉密专区管理、涉密设备管理、涉密载体管理、信息系统管理等方面给出了4大项20小项指引，引导企业建立完善防止商业秘密泄露的保密措施制度体系。

（四）保密信息管理。《指引》从信息存储、复制、流转、销毁等方面给出了4大项14小项指引，重点引导企业建立完善的信息管理制度，避免保密信息“失控”。

（五）商业秘密外部管理。《指引》从信息发布、商业合作、技术合作、跨境合作、并购重组等方面给出了5大项20小项指引，引导企业在对外商务活动、技术合作中对商业秘密实施有效管控。

（六）商业秘密侵权维权。《指引》从应急预案生效、侵权证据收集、侵权行为评估、维权途径确定等方面给出了4大项21小项指引，引导企业建立完善商业秘密被侵害后的应急处理机制，提高维权效能。

（七）合规风险防范。《指引》从入职人员背景调查、商业秘密权属查明、合作风险防范、研发记录存档、国际业务评估等方面给出了5大项15小项指引，引导企业建立防止侵犯他人商业秘密的制度体系，帮助企业避免陷入商业秘密侵权纠纷。

三、补充说明

一是本《指引》所列各项，均是在分析我市商业秘密刑事案件的基础上，以课题研究的方式总结提炼的，企业可以对照《指引》分析自身在商业秘密刑事保护体系建设工作存在的不足，制定更加详细的、适合于本企业的具体合规建设工作方案。

二是本《指引》虽已涉及125项具体指引，按照指引的要求，加强商业秘密刑事保护体建设，能够避免出现因结构性关键要素缺失，而无法得到刑事司法有效保护的遗憾，但难免还有不完善、未涉及的方面，《指引》只能作为企业加强商业秘密刑事保护体系合规建设工作的参考，企业全面落实《指引》建议不必然等于获得刑事保护。在具体的商业秘密案件中，是否能够获得刑事保护应当以事实为依据，以法律和司法解释为准绳，本《指引》不能作为定案依据引用。

出所：2023 年 4 月 27 日付け深セン市人民検察院ウェブサイト

https://mp.weixin.qq.com/s/zoSbLG4w5u9HOcNvPTvZKQ