

前 言

商业秘密作为企业核心无形资产，直接关系到企业的市场竞争力与可持续发展能力。当前科技创新加速、市场竞争加剧，商业秘密保护已成为企业合规经营、创新发展的关键环节。为切实提升系统企业商业秘密保护意识与实操能力，在市国资委、市知识产权保护中心指导下，由市国资委监管企业所属 7 家知识产权维权援助工作站牵头，联合外部专业力量共同编写了《企业商业秘密管理和保护问答集》。

本书坚持问题导向、实用导向，系统梳理现行有效法律法规，聚焦事前防范、事中管控、事后维权全流程，紧扣企业经营管理高频场景，将抽象法律条文转化为可操作、可落地、可执行的实务指引，旨在为企业法务、知识产权管理人员及一线业务人员提供简洁清晰、务实管用的工作参考。

编写过程中，编者力求内容准确、逻辑清晰，贴合实际需求，并广泛征求了司法机关、行业专家及企业实务人士意见。但由于商业秘密保护横跨法律、管理、技术等多个领域，且实践场景持续迭代，受限于编写周期与认知局限，本书难免存在考虑不周或表述不当之处，敬请各位读者包容谅解。期待本书能为国有企业筑牢商业秘密保护防线、提升核心竞争力、实现高质量发展贡献绵薄之力。

目 录

一、规范性法律文件

《中华人民共和国反不正当竞争法》（中华人民共和国主席令 第 50 号）	3
《商业秘密保护规定》（国家市场监督管理总局令第 126 号）	14
《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）	24

二、企业商业秘密管理和保护问答集

（一）商业秘密的内涵及界定	35
1 法律层面如何定义商业秘密？	35
2 商业秘密的秘密性、价值性、保密性三要件是什么关系？	35
3 如何证明信息符合商业秘密三要件？	36
4 商业秘密的权利主体有哪些？被许可方能否主张权利？	36
5 本企业商业秘密的内容应当由谁来决定？其法律边界与 最终认定依据是什么？	37
6 如何判断一段信息是否属于应保护的商业秘密？	37
7 行业常识或通用技能是商业秘密吗？	38

8	公司已申请专利的技术，相关过程资料还是商业秘密吗？	38
9	供应商或合作伙伴知道、或公司已公开披露的信息是否 还属于商业秘密？	39
10	公开信息加工改进后，能否成为商业秘密？	39
11	生产经营中失败的研发数据和阶段性成果受法律保护吗？	39
12	哪些信息属于技术秘密？	40
13	哪些信息不能作为技术秘密保护？	40
14	技术秘密与专利、著作权的区别是什么？企业该如何选 择申请专利或作为技术秘密保护？	41
(二) 企业商业秘密管理保护体系建设		41
15	如何对商业秘密进行分级分类管理？核心原则是什么？	41
16	搭建商业秘密保护体系的核心路径是什么？	42
17	企业必备的商业秘密保密制度包含哪些核心条款？是否 需要明确商业（技术）秘密清单及密级？	42
18	如何有效识别掌握核心商业秘密的关键岗位并进行管控？	42
19	涉密信息如何标注密级、限制接触范围？可采取哪些技 术防护措施？	43
20	数字化办公、远程办公场景下，技术保密措施有哪些？	43
21	涉密文件、代码、设备如何管控？电脑、服务器、云盘、 邮箱等如何防泄密？	44

22	保密要求如何嵌入研发流程？研发数据、图纸、模型、仿真文件存储、传输、权限如何有效受控？	44
23	企业并购、投融资过程中，如何保护商业秘密？	45
24	境外合作、数据跨境场景下，商业秘密如何保护？	45
25	日常经营中，如何建立并有效执行保密证据留存机制？	46
26	如何定期审查保密措施的落实情况？	46
27	如何建立合规隔离机制以避免无意中获取或使用未授权信息？	46
28	如何加强技术秘密及科技创新成果专门化管理，完善科技创新成果转化体系及配套制度？	47
(三) 落实“合理保密措施”及防止泄露风险		47
29	如何对入职、在职、离职人员做全流程保密管理？	47
30	实习生、临时工、劳务派遣人员是否需要签订保密协议？	48
31	对第三方劳务派遣、外包等接触保密信息的人员，如何确保保密措施落实？	48
32	员工是否需要签订保密协议、竞业限制协议？协议应包括哪些内容？	49
33	员工离职时的交接流程是什么？曾经接触的技术秘密文件如何处理？	49
34	针对合作方、外包方、访客，如何落实保密义务？	50

35	对签有竞业限制协议的离职人员，如何合法有效调查其是否入职竞争对手？	50
36	对外展示、参观、交流时，如何避免泄露技术秘密？	50
37	委托开发、测试、生产时，如何控制技术扩散？	51
38	展会、论文、专利申请中，如何避免无意中公开秘密？	51
39	涉密文件对外发送、合作共享有哪些风控要点？	52
40	外聘专家、合作研发、联合开发、高校合作的保密要求有哪些关键点？	52
41	与供应商、外包方合作时，除保密协议外，有哪些检查或审计方法核实其履行保密义务？	52
42	对外合作（如委托加工）中，如何防范合作方通过反向工程获取核心技术秘密？	53
43	使用开源代码，如何避免污染自有商业秘密？	53
44	如何有效避免离职研发人员带走方案、参数、文档的风险？	54
45	如何加强科技创新成果技术信息安全管控，健全技术秘密载体管理？	54
46	如果被诉侵权，如何以合法来源进行抗辩？	55
(四) 侵犯商业秘密行为认定		55
47	法律规定的侵犯商业秘密行为有哪些典型类型？电子侵入、云端窃密是否属于侵权？	55
48	未签订书面保密协议，是否负有商业秘密保密义务？	56

49	如何证明“技术秘密一旦泄露会造成损失”？	56
50	侵犯商业秘密的举证责任如何分配？企业举证难怎么办？	57
51	合作开发、委托开发中的技术秘密归属如何确定？	57
52	并购、投资、合作时，如何界定原有秘密与新增秘密？	57
53	侵犯商业秘密情节严重的认定标准是什么？	58
54	商业秘密民事侵权、行政违法、刑事犯罪的界限是什么？	58
55	哪些行为属于侵犯商业秘密的免责情形？	59
56	员工违反保密义务，企业能否直接开除并追责？	59
57	商业秘密被泄露后，如何固定电子证据？	59
58	员工泄露未在制度中明确列举的保密信息，如何证明该信息属于保密信息？如何证明泄密损失或对方获利？	60
59	员工离职后，哪些知识经验属合法可使用的自身技能？哪些属不能随意披露使用的商业秘密？	60
60	员工离职后入职竞品并使用原单位技术信息是否一定构成侵权？	61
61	核心研发员工离职后，能否以“成果含个人核心技能”为由在竞品处继续使用原履职期间主导的技术？	61
62	商业秘密被泄露但尚未造成实际损失，能否主张赔偿以及损失如何计算？	61
63	境外形成的商业秘密，在我国境内能否获得保护？	62

(五) 商业秘密保护途径与维权措施	62
64 商业秘密疑似泄露或被侵权，应启动哪些紧急应对流程？	62
65 企业如何主动监测商业秘密被侵犯，是否有成熟监测机构或技术手段？	63
66 商业秘密维权有哪些途径？刑事报案、行政举报、民事诉讼的优劣势及适用条件是什么？	63
67 提起商业秘密民事诉讼，管辖法院如何确定？	64
68 民事维权中可主张哪些赔偿？赔偿数额/损失/违法所得如何计算？	64
69 向市场监管部门投诉侵犯商业秘密，需准备哪些材料？行政投诉处理流程和时限是多久？	65
70 如何证明对方“获取、使用、披露”了企业的技术秘密？	65
71 维权中法院或行政主管部门最认可的证据类型有哪些？如何确保证据合法、真实、关联？	66
72 哪些情形下侵犯商业秘密会构成刑事犯罪？	66
73 企业可获得哪些商业秘密保护公共服务支持？	67
74 商业秘密与国家秘密重合时如何保护？	67
75 维权过程中，如何防止商业秘密二次泄露？	67
76 如何避免因自身保密措施不足导致败诉？	68
77 海外子公司（工厂）是否需要建立符合当地法规的商业秘密保护制度？	68
78 招录竞品离职员工，如何设计人事合规制度防范“共同侵权”及单位犯罪风险？	68

79	如何建立海外泄密应急预案、跨境响应机制?	69
80	商业秘密侵权纠纷中,当事人双方能否通过调解方式解决? 调解协议具有怎样的法律效力?	70

三、商业秘密保护典型案例集

(一)	商业秘密界定相关案例	73
(二)	管理保护体系建设相关案例	74
(三)	制度落实与日常风控相关案例	75
(四)	侵权行为及赔偿认定相关案例	76
(五)	刑事及行政维权相关案例	78

一、规范性法律文件

中华人民共和国反不正当竞争法

(1993年9月2日第八届全国人民代表大会常务委员会第三次会议通过 2017年11月4日第十二届全国人民代表大会常务委员会第三十次会议第一次修订 根据2019年4月23日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》修正 2025年6月27日第十四届全国人民代表大会常务委员会第十六次会议第二次修订)

目 录

- 第一章 总则
- 第二章 不正当竞争行为
- 第三章 对涉嫌不正当竞争行为的调查
- 第四章 法律责任
- 第五章 附则

第一章 总 则

第一条 为了促进社会主义市场经济健康发展，鼓励和保护公平竞争，预防和制止不正当竞争行为，保护经营者和消费者的合法权益，制定本法。

第二条 经营者在生产经营活动中，应当遵循自愿、平等、公平、诚信的原则，遵守法律和商业道德，公平参与市场竞争。

本法所称的不正当竞争行为，是指经营者在生产经营活动中，违反本法规定，扰乱市场竞争秩序，损害其他经营者或者消费者的合法权益的行为。

本法所称的经营者，是指从事商品生产、经营或者提供服务（以下所称商品包括服务）的自然人、法人和非法人组织。

第三条 反不正当竞争工作坚持中国共产党的领导。

国家健全完善反不正当竞争规则制度，加强反不正当竞争执法司法，维护市场竞争秩序，健全统一、开放、竞争、有序的市场体系。

国家建立健全公平竞争审查制度，依法加强公平竞争审查工作，保障各类经营者依法平等使用生产要素、公平参与市场竞争。

第四条 各级人民政府应当采取措施，预防和制止不正当竞争行为，为公平竞争创造良好的环境和条件。

国务院建立健全反不正当竞争工作协调机制，协调处理维护市场竞争秩序的重大问题。

第五条 县级以上人民政府履行市场监督管理职责的部门对不正当竞争行为进行监督检查；法律、行政法规规定由其他部门监督检查的，依照其规定。

第六条 国家鼓励、支持和保护一切组织和个人对不正当竞争行为进行社会监督。

国家机关及其工作人员不得支持、包庇不正当竞争行为。

行业组织应当加强行业自律，引导、规范本行业的经营者依法竞争，维护市场竞争秩序。

第二章 不正当竞争行为

第七条 经营者不得实施下列混淆行为，引人误认为是他人商品或者与他人存在特定联系：

（一）擅自使用与他人有一定影响的商品名称、包装、装潢等相同或者近似的标识；

（二）擅自使用他人有一定影响的名称（包括简称、字号等）、姓名（包括笔名、艺名、网名、译名等）；

（三）擅自使用他人有一定影响的域名主体部分、网站名称、网页、新媒体账号名称、应用程序名称或者图标等；

（四）其他足以引人误认为是他人商品或者与他人存在特定联系的混淆行为。

擅自将他人注册商标、未注册的驰名商标作为企业名称中的字号使用，或者将他人商品名称、企业名称（包括简称、字号等）、注册商标、未注册的驰名商标等设置为搜索关键词，引人误认为是他人商品或者与他人存在特定联系的，属于前款规定的混淆行为。

经营者不得帮助他人实施混淆行为。

第八条 经营者不得采用给予财物或者其他手段贿赂下列单位或者个人，以谋取交易机会或者竞争优势：

（一）交易相对方的工作人员；

（二）受交易相对方委托办理相关事务的单位或者个人；

（三）利用职权或者影响力影响交易的单位或者个人。

前款规定的单位和个人不得收受贿赂。

经营者在交易活动中，可以以明示方式向交易相对方支付折扣，或者向中间人支付佣金。经营者向交易相对方支付折扣、向中间人支付佣金的，应当如实入账。接受折扣、佣金的

经营者也应当如实入账。

经营者的工作人员进行贿赂的，应当认定为经营者的行为；但是，经营者有证据证明该工作人员的行为与为经营者谋取交易机会或者竞争优势无关的除外。

第九条 经营者不得对其商品的性能、功能、质量、销售状况、用户评价、曾获荣誉等作虚假或者引人误解的商业宣传，欺骗、误导消费者和其他经营者。

经营者不得通过组织虚假交易、虚假评价等方式，帮助其他经营者进行虚假或者引人误解的商业宣传。

第十条 经营者不得实施下列侵犯商业秘密的行为：

（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；

（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；

（四）教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密。

第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

本法所称的商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

第十一条 经营者进行有奖销售不得存在下列情形：

（一）所设奖的种类、兑奖条件、奖金金额或者奖品等有奖销售信息不明确，影响兑奖；

（二）有奖销售活动开始后，无正当理由变更所设奖的种类、兑奖条件、奖金金额或者奖品等有奖销售信息；

（三）采用谎称有奖或者故意让内定人员中奖等欺骗方式进行有奖销售；

（四）抽奖式的有奖销售，最高奖的金额超过五万元。

第十二条 经营者不得编造、传播或者指使他人编造、传播虚假信息或者误导性信息，损害其他经营者的商业信誉、商品声誉。

第十三条 经营者利用网络从事生产经营活动，应当遵守本法的各项规定。

经营者不得利用数据和算法、技术、平台规则等，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为：

（一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转；

（二）误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务；

（三）恶意对其他经营者合法提供的网络产品或者服务实施不兼容；

（四）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

经营者不得以欺诈、胁迫、避开或者破坏技术管理措施等不正当方式，获取、使用其他经营者合法持有的数据，损害其他经营者的合法权益，扰乱市场竞争秩序。

经营者不得滥用平台规则，直接或者指使他人对其他经营

者实施虚假交易、虚假评价或者恶意退货等行为，损害其他经营者的合法权益，扰乱市场竞争秩序。

第十四条 平台经营者不得强制或者变相强制平台内经营者按照其定价规则，以低于成本的价格销售商品，扰乱市场竞争秩序。

第十五条 大型企业等经营者不得滥用自身资金、技术、交易渠道、行业影响力等方面的优势地位，要求中小企业接受明显不合理的付款期限、方式、条件和违约责任等交易条件，拖欠中小企业的货物、工程、服务等账款。

第三章 对涉嫌不正当竞争行为的调查

第十六条 监督检查部门调查涉嫌不正当竞争行为，可以采取下列措施：

- （一）进入涉嫌不正当竞争行为的经营场所进行检查；
- （二）询问被调查的经营者、利害关系人及其他有关单位、个人，要求其说明有关情况或者提供与被调查行为有关的其他资料；
- （三）查询、复制与涉嫌不正当竞争行为有关的协议、账簿、单据、文件、记录、业务函电和其他资料；
- （四）查封、扣押与涉嫌不正当竞争行为有关的财物；
- （五）查询涉嫌不正当竞争行为的经营者的银行账户。

采取前款规定的措施，应当向监督检查部门主要负责人书面报告，并经批准。采取前款第四项、第五项规定的措施，应当向设区的市级以上人民政府监督检查部门主要负责人书面报告，并经批准。

监督检查部门调查涉嫌不正当竞争行为，应当遵守《中华人民共和国行政强制法》和其他有关法律、行政法规的规

定，并应当依法将查处结果及时向社会公开。

第十七条 监督检查部门调查涉嫌不正当竞争行为，被调查的经营者、利害关系人及其他有关单位、个人应当如实提供有关资料或者情况。

第十八条 经营者涉嫌违反本法规定的，监督检查部门可以对其有关负责人进行约谈，要求其说明情况、提出改进措施。

第十九条 监督检查部门及其工作人员对调查过程中知悉的商业秘密、个人隐私和个人信息依法负有保密义务。

第二十条 对涉嫌不正当竞争行为，任何单位和个人有权向监督检查部门举报，监督检查部门接到举报后应当依法及时处理。

监督检查部门应当向社会公开受理举报的电话、信箱或者电子邮件地址，并为举报人保密。对实名举报并提供相关事实和证据的，监督检查部门应当将处理结果及时告知举报人。

第二十一条 平台经营者应当在平台服务协议和交易规则中明确平台内公平竞争规则，建立不正当竞争举报投诉和纠纷处置机制，引导、规范平台内经营者依法公平竞争；发现平台内经营者实施不正当竞争行为的，应当及时依法采取必要的处置措施，保存有关记录，并按规定向平台经营者住所地县级以上人民政府监督检查部门报告。

第四章 法律责任

第二十二条 经营者违反本法规定，给他人造成损害的，应当依法承担民事责任。

经营者的合法权益受到不正当竞争行为损害的，可以向人民法院提起诉讼。

因不正当竞争行为受到损害的经营者的赔偿数额，按照其因被侵权所受到的实际损失或者侵权人因侵权所获得的利益确定。经营者故意实施侵犯商业秘密行为，情节严重的，可以在按照上述方法确定数额的一倍以上五倍以下确定赔偿数额。赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。

经营者违反本法第七条、第十条规定，权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益难以确定的，由人民法院根据侵权行为的情节判决给予权利人五百万元以下的赔偿。

第二十三条 经营者违反本法第七条规定实施混淆行为或者帮助他人实施混淆行为的，由监督检查部门责令停止违法行为，没收违法商品。违法经营额五万元以上的，可以并处违法经营额五倍以下的罚款；没有违法经营额或者违法经营额不足五万元的，可以并处二十五万元以下的罚款；情节严重的，并处吊销营业执照。

销售本法第七条规定的违法商品的，依照前款规定予以处罚；销售者不知道其销售的商品属于违法商品，能证明该商品是自己合法取得并说明提供者的，由监督检查部门责令停止销售，不予行政处罚。

经营者登记的名称违反本法第七条规定的，应当及时办理名称变更登记；名称变更前，由登记机关以统一社会信用代码代替其名称。

第二十四条 有关单位违反本法第八条规定贿赂他人或者收受贿赂的，由监督检查部门没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款，可以并处吊销营业执照。

经营者的法定代表人、主要负责人和直接责任人员对实施贿赂负有个人责任，以及有关个人收受贿赂的，由监督检查部

门没收违法所得，处一百万元以下的罚款。

第二十五条 经营者违反本法第九条规定对其商品作虚假或者引人误解的商业宣传，或者通过组织虚假交易、虚假评价等方式帮助其他经营者进行虚假或者引人误解的商业宣传的，由监督检查部门责令停止违法行为，处一百万元以下的罚款；情节严重的，处一百万元以上二百万元以下的罚款，可以并处吊销营业执照。

经营者违反本法第九条规定，属于发布虚假广告的，依照《中华人民共和国广告法》的规定处罚。

第二十六条 经营者以及其他自然人、法人和非法人组织违反本法第十条规定侵犯商业秘密的，由监督检查部门责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

第二十七条 经营者违反本法第十一条规定进行有奖销售的，由监督检查部门责令停止违法行为，处五万元以上五十万元以下的罚款。

第二十八条 经营者违反本法第十二条规定损害其他经营者商业信誉、商品声誉的，由监督检查部门责令停止违法行为、消除影响，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

第二十九条 经营者违反本法第十三条第二款、第三款、第四款规定利用网络从事不正当竞争的，由监督检查部门责令停止违法行为，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

第三十条 平台经营者违反本法第十四条规定强制或者变相强制平台内经营者以低于成本的价格销售商品的，由监督检查部门责令停止违法行为，处五万元以上五十万元以下的罚款；情节严重的，处五十万元以上二百万元以下的罚款。

第三十一条 经营者违反本法第十五条规定滥用自身优势地位的，由省级以上人民政府监督检查部门责令限期改正，逾期不改正的，处一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

第三十二条 经营者违反本法规定从事不正当竞争，有主动消除或者减轻违法行为危害后果等法定情形的，依法从轻或者减轻行政处罚；违法行为轻微并及时纠正，没有造成危害后果的，不予行政处罚。

第三十三条 经营者违反本法规定从事不正当竞争，受到行政处罚的，由监督检查部门记入信用记录，并依照有关法律、行政法规的规定予以公示。

第三十四条 经营者违反本法规定，应当承担民事责任、行政责任和刑事责任，其财产不足以支付的，优先用于承担民事责任。

第三十五条 妨害监督检查部门依照本法履行职责，拒绝、阻碍调查的，由监督检查部门责令改正，对个人可以处一万元以下的罚款，对单位可以处十万元以下的罚款。

第三十六条 当事人对监督检查部门作出的决定不服的，可以依法申请行政复议或者提起行政诉讼。

第三十七条 监督检查部门的工作人员滥用职权、玩忽职守、徇私舞弊或者泄露调查过程中知悉的商业秘密、个人隐私或者个人信息的，依法给予处分。

第三十八条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第三十九条 在侵犯商业秘密的民事审判程序中，商业秘密权利人提供初步证据，证明其已经对所主张的商业秘密采取保密措施，且合理表明商业秘密被侵犯，涉嫌侵权人应当证明权利人所主张的商业秘密不属于本法规定的商业秘密。

商业秘密权利人提供初步证据合理表明商业秘密被侵犯，且提供以下证据之一的，涉嫌侵权人应当证明其不存在侵犯商业秘密的行为：

（一）有证据表明涉嫌侵权人有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同；

（二）有证据表明商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险；

（三）有其他证据表明商业秘密被涉嫌侵权人侵犯。

第五章 附 则

第四十条 在中华人民共和国境外实施本法规定的不正当竞争行为，扰乱境内市场竞争秩序，损害境内经营者或者消费者的合法权益的，依照本法以及有关法律的规定处理。

第四十一条 本法自 2025 年 10 月 15 日起施行。

商业秘密保护规定

(2026 年 2 月 24 日国家市场监督管理总局令第 126 号公布 自 2026 年 6 月 1 日起施行)

第一条 为了加强商业秘密保护，维护公平竞争的市场秩序，根据《中华人民共和国反不正当竞争法》（以下简称反不正当竞争法），制定本规定。

第二条 经营者获取、披露、使用或者允许他人使用商业秘密应当遵循自愿、平等、公平、诚信的原则，遵守法律法规规章和商业道德，公平参与市场竞争。

本规定所称的经营者，是指从事商品生产、经营或者提供服务（以下所称商品包括服务）的自然人、法人和非法人组织。

第三条 国家市场监督管理总局负责组织、指导全国商业秘密行政保护工作。

县级以上地方市场监督管理部门负责本行政区域内商业秘密行政保护工作。

技术秘密案件一般由设区的市级以上市场监督管理部门管辖，根据工作需要，经国家市场监督管理总局同意，也可以由具有相应执法能力的县级市场监督管理部门管辖。

第四条 市场监督管理部门应当通过开展宣传解读、组织专项培训等方式，指导经营者建立健全商业秘密保护制度，强

化商业秘密保护意识和能力，推动商业秘密保护水平整体提升。

鼓励经营者建立健全商业秘密保护管理体系，根据自身行业特点、技术要求、竞争优势等，积极采取有效措施加强涉密要素的内部控制和合规管理，防范和制止侵犯商业秘密的行为。鼓励经营者创新商业秘密保护形式，通过认证、存证等方式强化商业秘密保护。

行业组织应当加强行业自律，通过制定本行业商业秘密保护规范、合规指引等方式，引导、规范本行业的经营者依法竞争，维护市场竞争秩序。

第五条 本规定所称的商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

与技术有关的结构、原料、配方、材料、样品、样式、工艺、方法、数据、算法、计算机程序、代码等信息，属于第一款所称的技术信息。

与经营活动有关的创意、管理、销售、财务、计划、样本、客户信息、数据等信息，属于第一款所称的经营信息。其中，客户信息包括客户的名称（姓名）、地址、联系方式以及交易习惯、意向、内容等信息。

第六条 本规定所称的不为公众所知悉，是指在涉嫌侵犯商业秘密的行为发生时，有关商业信息不为其所属领域的相关人员普遍知悉和容易获得。

下列情形属于有关商业信息为公众所知悉：

- （一）该信息在所属领域属于一般常识或者行业惯例；
- （二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得；

（三）该信息已经在公开出版物或者其他媒体上公开披露；

（四）该信息已通过公开的报告会、展览等方式公开；

（五）所属领域的相关人员从其他公开渠道可以获得该信息。

将为公众所知悉的有关商业信息进行整理、改进、加工后形成新信息，符合第一款规定的，属于不为公众所知悉的情形。

第七条 本规定所称的具有商业价值，是指商业信息具有现实的或者潜在的价值，能为权利人带来资产增加、营业收入或者利润增长、用户数量增长、成本费用降低、研发时间缩短、交易机会增加、商业信誉或者商品声誉提升等商业利益或者竞争优势。

生产经营活动中形成的阶段性成果或者失败的实验数据、技术方案等符合第一款规定的，属于具有商业价值的情形。

第八条 本规定所称的权利人，是指商业秘密所有人和经商业秘密所有人许可、授权的商业秘密被许可人、被授权人。

第九条 本规定所称的权利人采取相应保密措施，是指权利人为防止商业秘密泄露，采取与商业秘密及其载体的性质、商业秘密的商业价值等因素相适应的合理保密措施。

下列情形属于权利人采取的相应保密措施：

（一）签订保密协议或者在合同中约定保密义务；

（二）通过建立规章制度、开展培训、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求；

（三）禁止或者限制进入涉密的厂房、车间、实验室、办公室等生产经营场所或者对其进行区管理；

（四）针对远程办公、跨境协作等场景，采取权限分级、

数据脱敏、操作日志留痕等技术保密措施；

（五）以标记、分类、隔离、加密、封存、限制能够接触或者获取商业秘密及其载体的人员范围等方式，对商业秘密及其载体进行区分管理；

（六）对能够接触、获取商业秘密的计算机设备、网络设备、存储设备等，采取禁止或者限制使用、访问、存储、复制等措施；

（七）要求离职员工登记、返还、清除、销毁其接触、获取的商业秘密及其载体，继续承担保密义务；

（八）采取其他合理保密措施。

第十条 经营者不得以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密。

下列情形属于本规定所称的不正当手段：

（一）未经授权或者超出授权范围，擅自接触、占有或者复制由权利人控制下的，包含商业秘密或者能从中推导出商业秘密的文件、物品、材料、原料等载体；

（二）通过提供财物或者其他财产性利益、人身威胁等方式，贿赂、胁迫、欺骗权利人的员工、前员工或者其他单位、个人为其获取商业秘密；

（三）未经授权或者超出授权范围，擅自进入权利人的数字化办公系统、服务器、邮箱、云盘、应用账户等，或者通过设置恶意程序、漏洞攻击等技术手段获取商业秘密；

（四）未经授权、超出授权范围或者授权期限届满后，擅自将商业秘密下载或者传输至不受权利人控制的电子邮箱、云盘等网络存储空间或者电子设备；

（五）其他获取权利人商业秘密的不正当手段。

第十一条 经营者不得披露、使用或者允许他人使用以不正当手段获取的权利人的商业秘密。

本规定所称的披露，是指将商业秘密泄露给权利人之外的第三人，或者将商业秘密公之于众，为相关公众普遍知悉或者容易获得。

本规定所称的使用，是指直接使用商业秘密，或者对商业秘密进行修改、改进后使用，或者根据商业秘密调整、改进有关生产经营活动。

第十二条 经营者不得违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密。

保密义务或者权利人有关保守商业秘密的要求一般包括下列情形：

（一）在劳动合同、保密合同、买卖合同等合同中约定保守商业秘密；

（二）没有合同约定，但根据合同的性质、目的和交易习惯、商业道德等，遵循诚信原则，负有保守商业秘密的义务；

（三）权利人对知悉商业秘密的有关主体提出保密要求，有关主体包括但不限于通过合同关系知悉该商业秘密，以及通过参与研发、生产、检验、认证等活动知悉该商业秘密的主体；

（四）没有合同约定，但权利人通过规章制度或者合理的保密措施，对员工、前员工、合作方等明确提出保守商业秘密的要求；

（五）其他负有保密义务或者权利人提出有关保守商业秘密要求的情形。

第十三条 经营者不得教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

下列情形属于教唆、引诱、帮助他人侵犯商业秘密的

行为：

（一）以明示或者暗示的方式，怂恿、指使他人侵犯商业秘密；

（二）以明示或者暗示的方式，通过物质奖励或者职位许诺等非物质奖励诱导他人侵犯商业秘密；

（三）明知或者应知他人侵犯商业秘密，仍为其提供资金、技术、设备等便利条件；

（四）其他教唆、引诱、帮助他人侵犯商业秘密的行为。

第十四条 经营者以外的其他自然人、法人和非法人组织实施本规定第十条至第十三条规定的违法行为的，视为侵犯商业秘密。

第三人明知或者应知商业秘密权利人的员工、前员工、合作方或者其他单位、个人实施本规定第十条至第十三条规定的违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

判断第三人是否明知或者应知，应当综合考虑有关商业信息的保密程度、获取渠道与方式的合理性、交易价格、第三人与商业秘密权利人的关系、行业惯例等因素。

第十五条 下列行为一般不属于侵犯商业秘密的行为：

（一）独立发现或者自行研发；

（二）对从公开渠道取得的产品进行拆卸、测绘、分析等获得该产品的有关技术信息；

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

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

（五）其他不属于侵犯商业秘密的行为。

第十六条 鼓励、支持和保护一切组织和个人对侵犯商业秘密的行为进行社会监督。市场监督管理部门应当对举报人和协助查处侵犯商业秘密行为的组织和个人的信息予以保密。

第十七条 权利人认为其商业秘密受到侵犯的，可以向市场监督管理部门举报。

权利人举报时，应当提供其商业信息属于商业秘密的初步证据材料以及该商业秘密涉嫌被侵犯的具体线索，并对举报内容的真实性负责。市场监督管理部门根据工作需要，可以要求举报人补充举报材料。

任何组织和个人不得捏造侵犯商业秘密的事实诬陷他人、实施敲诈勒索，不得滥用举报权利扰乱市场竞争秩序和市场监督管理秩序。

第十八条 权利人的商业信息属于商业秘密的初步证据材料一般包括下列内容：

- （一）商业信息的形成过程和形成时间；
- （二）商业信息不为公众所知悉或者不属于本规定第六条第二款所列情形；
- （三）商业信息的商业价值；
- （四）权利人对该商业信息所采取的保密措施；
- （五）其他能够证明权利人的商业信息属于商业秘密的证据材料。

下列线索一般可以作为商业秘密涉嫌被侵犯的具体线索：

- （一）表明涉嫌侵犯商业秘密的人（以下简称侵权人）有渠道或者机会获取商业秘密的线索；
- （二）表明商业秘密的保密措施被涉嫌侵权人以不正当手段破坏的线索；
- （三）表明商业秘密已被涉嫌侵权人实际获取的线索；

（四）表明商业秘密已被涉嫌侵权人披露、使用或者有被披露、使用风险的线索；

（五）其他表明商业秘密被涉嫌侵权人侵犯的线索。

第十九条 市场监督管理部门收到举报线索后，应当依法进行核查，并决定是否立案。

经核查，符合下列条件的，应当立案：

（一）有证据初步证明存在侵犯商业秘密的行为，并依法应当给予行政处罚；

（二）属于本部门管辖；

（三）在给予行政处罚的法定期限内。

第二十条 涉嫌侵权人、利害关系人及其他有关单位、个人应当如实向市场监督管理部门提供有关资料或者情况。

有证据证明涉嫌侵权人所使用的信息与权利人主张的商业秘密实质相同，且涉嫌侵权人有获取商业秘密的条件，市场监督管理部门可以认定涉嫌侵权人存在侵犯商业秘密的行为，但有证据证明涉嫌侵权人所使用的信息是合法获得或者使用的除外。

第二十一条 市场监督管理部门及其工作人员对调查过程中知悉的商业秘密依法负有保密义务，不得违法披露、使用或者允许他人使用权利人的商业秘密。

市场监督管理部门依法公开行政处罚决定时，不得公开涉及商业秘密的内容。

第二十二条 权利人、涉嫌侵权人可以委托具有法定资质的鉴定机构，对权利人的信息是否为公众所知悉、涉嫌侵权人所使用的信息与权利人的信息是否实质相同等专门事项进行鉴定，或者委托有专门知识的人，对上述事项出具专业意见，并将有关鉴定结果或者专业意见提交市场监督管理部门。

第二十三条 市场监督管理部门调查涉嫌侵犯商业秘密行

为，可以采取下列措施：

（一）进入涉嫌侵犯商业秘密行为的经营场所进行检查；

（二）询问被调查的涉嫌侵权人、利害关系人及其他有关单位、个人，要求其说明有关情况或者提供与被调查行为有关的其他资料；

（三）查询、复制与涉嫌侵犯商业秘密行为有关的协议、账簿、单据、文件、记录、业务函电和其他资料；

（四）查封、扣押与涉嫌侵犯商业秘密行为有关的财物；

（五）查询涉嫌侵犯商业秘密行为的经营者的银行账户。

采取第一款规定的措施，应当向市场监督管理部门主要负责人书面报告，并经批准。采取第一款第四项、第五项规定的措施，应当向设区的市级以上市场监督管理部门主要负责人书面报告，并经批准。

市场监督管理部门及其工作人员依法开展调查或者要求协助调查，应当避免或者尽量减少对经营者正常生产经营活动产生影响。

第二十四条 违反本规定侵犯商业秘密的，由县级以上市场监督管理部门依照反不正当竞争法第二十六条的规定，责令停止违法行为，没收违法所得，处十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。

第二十五条 依照反不正当竞争法第二十六条规定责令停止违法行为时，责令停止违法行为的时间一般应当持续至有关商业信息不再构成商业秘密为止。

责令停止违法行为一般包括：

（一）责令侵权人停止使用权利人的商业秘密，但权利人同意的除外；

（二）责令侵权人将商业秘密载体返还权利人或者销毁；

（三）责令侵权人销毁含有商业秘密的侵权产品或者中间

品，但权利人同意采取收购、销售等其他处理方式的除外；

（四）责令侵权人清除其获取的权利人的商业秘密；

（五）其他责令停止侵犯权利人商业秘密的行为。

第二十六条 下列情形属于反不正当竞争法第二十六条所称的情节严重：

（一）造成权利人直接损失数额较大；

（二）对权利人的生产经营活动造成重大不利影响；

（三）危害国家利益、社会公共利益；

（四）二年内因侵犯商业秘密受到行政处罚后，再次实施侵犯商业秘密行为；

（五）其他情节严重的情形。

第二十七条 违反本规定，涉嫌犯罪的，依法移送司法机关追究刑事责任。

第二十八条 本规定所称商业信息属于国家秘密的，依照《中华人民共和国保守国家秘密法》的规定进行保护。

第二十九条 在中华人民共和国境外实施侵犯商业秘密行为，扰乱境内市场竞争秩序，损害境内经营者合法权益的，依照反不正当竞争法以及有关法律的规定处理。

第三十条 法律、行政法规规定由其他部门对侵犯商业秘密行为进行监督检查的，依照其规定执行。

第三十一条 本规定自 2026 年 6 月 1 日起施行。1995 年 11 月 23 日原国家工商行政管理局令第 41 号公布的《关于禁止侵犯商业秘密行为的若干规定》同时废止。

中华人民共和国最高人民法院

公 告

《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》已于2020年8月24日由最高人民法院审判委员会第1810次会议通过，现予公布，自2020年9月12日起施行。

2020年9月10日

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

为正确审理侵犯商业秘密民事案件，根据《中华人民共和国反不正当竞争法》《中华人民共和国民事诉讼法》等有关规定，结合审判实际，制定本规定。

第一条 与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息，人民法院可以认定构成反不正当竞争法第九条第四款所称的技术信息。

与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息，人民法院可以认定构成反不正当竞争法第九条第四款所称的经营信息。

前款所称的客户信息，包括客户的名称、地址、联系方式

以及交易习惯、意向、内容等信息。

第二条 当事人仅以与特定客户保持长期稳定交易关系为由，主张该特定客户属于商业秘密的，人民法院不予支持。

客户基于对员工个人的信赖而与该员工所在单位进行交易，该员工离职后，能够证明客户自愿选择与该员工或者该员工所在的新单位进行交易的，人民法院应当认定该员工没有采用不正当手段获取权利人的商业秘密。

第三条 权利人请求保护的信息在被诉侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得的，人民法院应当认定为反不正当竞争法第九条第四款所称的不为公众所知悉。

第四条 具有下列情形之一的，人民法院可以认定有关信息为公众所知悉：

（一）该信息在所属领域属于一般常识或者行业惯例的；

（二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；

（三）该信息已经在公开出版物或者其他媒体上公开披露的；

（四）该信息已通过公开的报告会、展览等方式公开的；

（五）所属领域的相关人员从其他公开渠道可以获得该信息的。

将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合本规定第三条规定的，应当认定该新信息不为公众所知悉。

第五条 权利人为防止商业秘密泄露，在被诉侵权行为发生以前所采取的合理保密措施，人民法院应当认定为反不正当竞争法第九条第四款所称的相应保密措施。

人民法院应当根据商业秘密及其载体的性质、商业秘密的

商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，认定权利人是否采取了相应保密措施。

第六条 具有下列情形之一，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权利人采取了相应保密措施：

（一）签订保密协议或者在合同中约定保密义务的；

（二）通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；

（三）对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；

（四）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；

（五）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；

（六）要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；

（七）采取其他合理保密措施的。

第七条 权利人请求保护的信息因不为公众所知悉而具有现实的或者潜在的商业价值的，人民法院经审查可以认定为反不正当竞争法第九条第四款所称的具有商业价值。

生产经营活动中形成的阶段性成果符合前款规定的，人民法院经审查可以认定该成果具有商业价值。

第八条 被诉侵权人以违反法律规定或者公认的商业道德的方式获取权利人的商业秘密的，人民法院应当认定属于反不正当竞争法第九条第一款所称的以其他不正当手段获取权利人

的商业秘密。

第九条 被诉侵权人在生产经营活动中直接使用商业秘密，或者对商业秘密进行修改、改进后使用，或者根据商业秘密调整、优化、改进有关生产经营活动的，人民法院应当认定属于反不正当竞争法第九条所称的使用商业秘密。

第十条 当事人根据法律规定或者合同约定所承担的保密义务，人民法院应当认定属于反不正当竞争法第九条第一款所称的保密义务。

当事人未在合同中约定保密义务，但根据诚信原则以及合同的性质、目的、缔约过程、交易习惯等，被诉侵权人知道或者应当知道其获取的信息属于权利人的商业秘密的，人民法院应当认定被诉侵权人对其获取的商业秘密承担保密义务。

第十一条 法人、非法人组织的经营、管理人员以及具有劳动关系的其他人员，人民法院可以认定为反不正当竞争法第九条第三款所称的员工、前员工。

第十二条 人民法院认定员工、前员工是否有渠道或者机会获取权利人的商业秘密，可以考虑与其有关的下列因素：

- （一）职务、职责、权限；
- （二）承担本职工作或者单位分配的任务；
- （三）参与和商业秘密有关的生产经营活动的具体情形；
- （四）是否保管、使用、存储、复制、控制或者以其他方式接触、获取商业秘密及其载体；
- （五）需要考虑的其他因素。

第十三条 被诉侵权信息与商业秘密不存在实质性区别的，人民法院可以认定被诉侵权信息与商业秘密构成反不正当竞争法第三十二条第二款所称的实质上相同。

人民法院认定是否构成前款所称的实质上相同，可以考虑下列因素：

（一）被诉侵权信息与商业秘密的异同程度；

（二）所属领域的相关人员在被诉侵权行为发生时是否容易想到被诉侵权信息与商业秘密的区别；

（三）被诉侵权信息与商业秘密的用途、使用方式、目的、效果等是否具有实质性差异；

（四）公有领域中与商业秘密相关信息的情况；

（五）需要考虑的其他因素。

第十四条 通过自行开发研制或者反向工程获得被诉侵权信息的，人民法院应当认定不属于反不正当竞争法第九条规定的侵犯商业秘密行为。

前款所称的反向工程，是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。

被诉侵权人以不正当手段获取权利人的商业秘密后，又以反向工程为由主张未侵犯商业秘密的，人民法院不予支持。

第十五条 被申请人试图或者已经以不正当手段获取、披露、使用或者允许他人使用权利人所主张的商业秘密，不采取行为保全措施会使判决难以执行或者造成当事人其他损害，或者将会使权利人的合法权益受到难以弥补的损害的，人民法院可以依法裁定采取行为保全措施。

前款规定的情形属于民事诉讼法第一百条、第一百零一条所称情况紧急的，人民法院应当在四十八小时内作出裁定。

第十六条 经营者以外的其他自然人、法人和非法人组织侵犯商业秘密，权利人依据反不正当竞争法第十七条的规定主张侵权人应当承担的民事责任的，人民法院应予支持。

第十七条 人民法院对于侵犯商业秘密行为判决停止侵害的民事责任时，停止侵害的时间一般应当持续到该商业秘密已为公众所知悉时为止。

依照前款规定判决停止侵害的时间明显不合理的，人民法院可以在依法保护权利人的商业秘密竞争优势的情况下，判决侵权人在一定期限或者范围内停止使用该商业秘密。

第十八条 权利人请求判决侵权人返还或者销毁商业秘密载体，清除其控制的商业秘密信息的，人民法院一般应予以支持。

第十九条 因侵权行为导致商业秘密为公众所知悉的，人民法院依法确定赔偿数额时，可以考虑商业秘密的商业价值。

人民法院认定前款所称的商业价值，应当考虑研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素。

第二十条 权利人请求参照商业秘密许可使用费确定因被侵权所受到的实际损失的，人民法院可以根据许可的性质、内容、实际履行情况以及侵权行为的性质、情节、后果等因素确定。

人民法院依照反不正当竞争法第十七条第四款确定赔偿数额的，可以考虑商业秘密的性质、商业价值、研究开发成本、创新程度、能带来的竞争优势以及侵权人的主观过错、侵权行为的性质、情节、后果等因素。

第二十一条 对于涉及当事人或者案外人的商业秘密的证据、材料，当事人或者案外人书面申请人民法院采取保密措施的，人民法院应当在保全、证据交换、质证、委托鉴定、询问、庭审等诉讼活动中采取必要的保密措施。

违反前款所称的保密措施的要求，擅自披露商业秘密或者在诉讼活动之外使用或者允许他人使用在诉讼中接触、获取的商业秘密的，应当依法承担民事责任。构成民事诉讼法第一百一十一条规定情形的，人民法院可以依法采取强制措施。构成犯罪的，依法追究刑事责任。

第二十二条 人民法院审理侵犯商业秘密民事案件时，对在侵犯商业秘密犯罪刑事诉讼程序中形成的证据，应当按照法定程序，全面、客观地审查。

由公安机关、检察机关或者人民法院保存的与被诉侵权行为具有关联性的证据，侵犯商业秘密民事案件的当事人及其诉讼代理人因客观原因不能自行收集，申请调查收集的，人民法院应当准许，但可能影响正在进行的刑事诉讼程序的除外。

第二十三条 当事人主张依据生效刑事裁判认定的实际损失或者违法所得确定涉及同一侵犯商业秘密行为的民事案件赔偿数额的，人民法院应予支持。

第二十四条 权利人已经提供侵权人因侵权所获得的利益的初步证据，但与侵犯商业秘密行为相关的账簿、资料由侵权人掌握的，人民法院可以根据权利人的申请，责令侵权人提供该账簿、资料。侵权人无正当理由拒不提供或者不如实提供的，人民法院可以根据权利人的主张和提供的证据认定侵权人因侵权所获得的利益。

第二十五条 当事人以涉及同一被诉侵犯商业秘密行为的刑事案件尚未审结为由，请求中止审理侵犯商业秘密民事案件，人民法院在听取当事人意见后认为必须以该刑事案件的审理结果为依据的，应予支持。

第二十六条 对于侵犯商业秘密行为，商业秘密独占使用许可合同的被许可人提起诉讼的，人民法院应当依法受理。

排他使用许可合同的被许可人和权利人共同提起诉讼，或者在权利人不起诉的情况下自行提起诉讼的，人民法院应当依法受理。

普通使用许可合同的被许可人和权利人共同提起诉讼，或者经权利人书面授权单独提起诉讼的，人民法院应当依法受理。

第二十七条 权利人应当在一审法庭辩论结束前明确所主张的商业秘密具体内容。仅能明确部分的，人民法院对该明确的部分进行审理。

权利人在第二审程序中另行主张其在一审中未明确的商业秘密具体内容的，第二审人民法院可以根据当事人自愿的原则就与该商业秘密具体内容有关的诉讼请求进行调解；调解不成的，告知当事人另行起诉。双方当事人均同意由第二审人民法院一并审理的，第二审人民法院可以一并裁判。

第二十八条 人民法院审理侵犯商业秘密民事案件，适用被诉侵权行为发生时的法律。被诉侵权行为在法律修改之前已经发生且持续到法律修改之后的，适用修改后的法律。

第二十九条 本规定自 2020 年 9 月 12 日起施行。最高人民法院以前发布的相关司法解释与本规定不一致的，以本规定为准。

本规定施行后，人民法院正在审理的一审、二审案件适用本规定；施行前已经作出生效裁判的案件，不适用本规定再审。

二、企业商业秘密管理和保护问答集

（一）商业秘密的内涵及界定

1 法律层面如何定义商业秘密？

答：商业秘密是市场经济活动中受法律严格保护的核心商业信息，必须同时满足三项法定构成条件：（1）不为公众所知悉，即信息在涉嫌侵犯商业秘密的行为发生时不属于所属领域相关人员普遍知晓、容易获得的内容，具有秘密性；（2）具有商业价值，信息能给权利人带来现实或潜在的经济利益、竞争优势，包括盈利、成本节约、市场领先等价值；（3）权利人基于保密意愿，通过签订保密协议、建立规章制度、针对涉密设备及场所进行技术隔离或物理管控等方式，采取与商业秘密及其载体的性质、商业秘密的商业价值等因素相适应的合理保密措施。只有同时具备秘密性、价值性、保密性的技术信息、经营信息等商业信息，才能被认定为法律意义上的商业秘密。

法律依据：《中华人民共和国反不正当竞争法》第十条；《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》第一条、第三条、第五条、第七条；《商业秘密保护规定》第五条。

2 商业秘密的秘密性、价值性、保密性三要件是什么关系？

答：三要件是并列共存、缺一不可、逻辑递进、互为支撑的关系。秘密性是前提基础，信息若在涉嫌侵犯商业秘密行为发生前已公开，无论是否有价值、是否采取保密措施，都无法成为商业秘密；价值性是核心目的，无商业价值的信息，即便保密也不具备法律保护的必要性；保密性是法律保护的关键，权利人未采取合理保密措施，则因不满足法定构成要件而不能

获得法律保护。实践中，司法、行政机关会同时审查三项要件，任何一项不满足，均不构成商业秘密。

法律依据：《中华人民共和国反不正当竞争法》第十条；《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》第三条至第十二条；《商业秘密保护规定》第五条、第六条、第七条、第九条。

3 如何证明信息符合商业秘密三要件？

答：需围绕秘密性、价值性、保密性分别举证，形成完整证据链。秘密性：可提交行业检索报告、公开渠道查询记录等，也可以委托具有法定资质的鉴定机构进行鉴定，或者委托有专门知识的人出具专业意见，证明信息不为其所属领域的相关人员普遍知悉和容易获得；价值性：可提交研发成本、盈利数据、合同订单、市场份额、竞争优势分析等，证明信息能带来经济利益或竞争优势；保密性：可提交保密制度、保密协议、密级标注、权限管控记录、培训记录、载体管理台账等，证明已采取相应、合理的保密措施。三方面证据相互印证，可用于认定信息符合商业秘密法定要件。

法律依据：《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》第三条至第十二条；《商业秘密保护规定》第五条、第六条、第七条、第九条。

4 商业秘密的权利主体有哪些？被许可方能否主张权利？

答：商业秘密权利主体包括原始权利人和继受权利人。原始权利人主要是自主研发、形成商业秘密的企业、自然人、其他组织；继受权利人包括通过转让、继承、许可等方式获得权

利的主体。独占被许可方享有独立维权权利，可单独提起诉讼、行政举报；排他被许可方在权利人不维权时，可独立主张权利；普通被许可方需经权利人明确授权，方可代为主张权利。

法律依据：《中华人民共和国民法典》第一百二十三条；《商业秘密保护规定》第八条。

5 本企业商业秘密的内容应当由谁来决定？其法律边界与最终认定依据是什么？

答：企业可自主成立商业秘密认定工作组，由法务、研发、经营、管理等部门共同制定商业秘密清单，明确保护范围，仅限符合“非公知、有价值、已保密”的技术信息、经营信息，排除公知常识、通用技能、法定公开信息等。

企业内部清单仅为企业内部管理依据，司法、行政机关以《反不正当竞争法》规定的三要件为最终认定标准，不以企业单方列举为唯一依据。

法律依据：《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》第一条；《商业秘密保护规定》第五条、第九条。

6 如何判断一段信息是否属于应保护的商业秘密？

答：可采用“要件审查+排除情形筛查”方式进行判断。首先，审查是否不为公众所知悉、是否具有商业价值、以及是否采取合理保密措施；其次，排除行业常识、通用技能、已公开信息、个人技能、违法信息等。同时满足三要件，且不属于排除情形的信息，均属于应保护的商业秘密，应纳入保密管理范围。

法律依据：《中华人民共和国反不正当竞争法》第十条；《商业秘密保护规定》第五条、第六条、第七条、第九条、第十五条。

7 行业常识或通用技能是商业秘密吗？

答：行业常识、通用技能不属于商业秘密。因为行业常识是行业内普遍知晓、公开可得的信息，不满足“不为公众所知悉”的秘密性要件；通用技能是劳动者通过学习、培训、工作积累的基础能力，属于个人知识储备，并非企业专属商业信息。法律明确将公知常识、通用技能排除在商业秘密保护范围之外，允许从业人员自由使用，一般不构成侵权。

法律依据：《商业秘密保护规定》第十五条；《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》第四条。

8 公司已申请专利的技术，相关过程资料还是商业秘密吗？

答：已申请专利的技术，公开部分不属于商业秘密，未公开过程资料仍可作为商业秘密保护。专利以“公开换保护”，申请文件中披露的技术方案、参数、结构等内容已处于公开状态，丧失秘密性。但是，专利申请过程中未公开的实验数据、配方比例、工艺步骤、中间参数、失败试验记录、优化方案等，仍具备非公知性、商业价值，且企业采取保密措施的，完全符合商业秘密要件，受法律保护。

法律依据：《中华人民共和国专利法》第二十六条、第三十四条；《商业秘密保护规定》第六条、第七条。

9 供应商或合作伙伴知道、或公司已公开披露的信息

是否还属于商业秘密？

答：仅特定主体知悉，不是商业秘密认定的唯一依据，还需区分定向披露和完全公开两种情形。向供应商、合作伙伴等特定对象披露，且签订保密协议、约定保密义务、限制使用范围的，信息未进入公有领域，仍属于商业秘密。但是，向社会公众完全公开（如官网发布、媒体报道、展会公开等），或向不特定对象无保密义务披露的，信息丧失秘密性，不再属于商业秘密。

法律依据：《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》第四条；《商业秘密保护规定》第五条、第六条。

10 公开信息加工改进后，能否成为商业秘密？

答：公开信息经深度加工、整合、优化、创新后，可以成为商业秘密。原始公开信息属于公知内容，但企业投入人力、物力、技术进行改进，形成独特的、非公知的技术方案、经营策略、数据模型后，新信息具备秘密性；改进后的信息能为企业带来竞争优势，具备价值性；企业采取保密措施的，具备保密性；满足三要件的要求，可以成为商业秘密。

法律依据：《商业秘密保护规定》第六条。

11 生产经营中失败的研发数据和阶段性成果受法律保护吗？

答：失败的研发数据、阶段性成果可能属于商业秘密，受法律保护。此类信息如未公开，具备秘密性；失败数据可避免

重复研发、节约成本、缩短周期，阶段性成果是后续研发的基础，均具有现实商业价值和竞争优势；同时，为获得保护，企业如采取了相关保密措施，也具备保密性。此时，可作为商业秘密受法律保护。

法律依据：《商业秘密保护规定》第五条、第七条。

12 哪些信息属于技术秘密？

答：与技术有关的结构、原料、配方、材料、样品、样式、工艺、方法、数据、算法、计算机程序、代码等信息，属于技术信息，前述技术信息如果是企业未公开的、具有价值的，且采取了保密措施的，可构成技术秘密。

法律依据：《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》第一条；《商业秘密保护规定》第五条。

13 哪些信息不能作为技术秘密保护？

答：以下信息不得作为技术秘密保护：（1）已公开信息：专利公开内容、论文发表、官网披露、行业公开发布的信息等；（2）公知常识与通用技能：行业基础常识、通用操作方法、基础专业技能等；（3）无价值信息：无法带来经济利益、竞争优势的无效信息。此类信息不满足三要件，不属于保护范围。

法律依据：《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》第四条；《商业秘密保护规定》第六条、第十五条。

14 技术秘密与专利、著作权的区别是什么？企业该如何选择申请专利或作为技术秘密保护？

答：三者的核心区别包括：专利保护技术方案或设计，以公开换取保护，保护期限固定，排他性强，禁止他人使用；著作权则保护思想的表达形式，不保护思想本身，自动取得保护，保护期限较长；技术秘密保护非公知技术信息，不公开、无固定保护期限，依靠保密措施维持权利。

企业可以根据相关技术信息的特点来选择保护方式，对于易反向工程、易复制、结构型技术，申请专利以获得法定排他保护；对于核心配方、工艺、算法、模型等难以反向工程的技术，则以技术秘密的形式长期保密保持优势；对于软件代码等，可同时采取著作权登记以及技术秘密来保护。

法律依据：《中华人民共和国专利法》第二条、第四十二条；《中华人民共和国著作权法》第二条、第三条、第二十二条、第二十三条；《中华人民共和国反不正当竞争法》第十条。

（二）企业商业秘密管理保护体系建设

15 如何对商业秘密进行分级分类管理？核心原则是什么？

答：分级：核心商业秘密，影响企业生存发展的核心技术/经营信息、重要秘密，影响企业竞争优势的关键信息；普通商业秘密，日常经营中需保密的普通信息。分类：技术秘密（研发、技术、数据等）、经营秘密（客户、报价、财务、策略等）。

核心原则：最小授权原则、按需知悉原则、全程留痕原则、动态更新原则，即仅向必要岗位开放必要权限，定期调整密级与范围。

法律依据：《商业秘密保护规定》第四条、第九条。

16 搭建商业秘密保护体系的核心路径是什么？

答：采用“全流程闭环管理”路径，可以包括：（1）制定保密制度、协议、流程；（2）定密：识别商业秘密范围，明确清单；（3）分级分类：划分密级与信息类型；（4）人员管控：关键岗位、涉密人员全周期管理；（5）技术防护：加密、权限、水印、审计等技术手段；（6）物理管控：涉密区域、设备、载体管理；（7）流程嵌入：将保密要求融入研发、生产、合作、离职等流程；（8）审计监督：定期检查保密措施落实情况；（9）应急处置：泄密后快速响应、止损取证；（10）维权追责：通过民事、行政、刑事途径追责。

法律依据：《商业秘密保护规定》第九条。

17 企业必备的商业秘密保密制度包含哪些核心条款？

是否需要明确商业（技术）秘密清单及密级？

答：必备核心条款包括：（1）商业秘密定义与范围；（2）密级划分与标注规则；（3）涉密人员管理与权限；（4）涉密载体（纸质/电子）管理；（5）存储、传输、外发审批流程；（6）研发、合作、参观、离职等场景保密要求；（7）保密培训与考核；（8）泄密责任与奖惩。

秘密清单和密级是证明“合理保密措施”的核心依据，未明确清单密级，司法、行政机关可能认定未采取有效保密措施，可能导致权利不被保护。因此，有必要予以明确。

法律依据：《商业秘密保护规定》第九条。

18 如何有效识别掌握核心商业秘密的关键岗位并进行

管控？

答：可以根据岗位接触信息的密级、范围、重要性，列出

关键岗位清单，如研发负责人、核心工程师、财务总监、销售总监、高管等。管控措施可以包括：（1）协议管控：签订保密协议、竞业限制协议；（2）权限管控：最小授权、分级访问、全程留痕；（3）培训管控：定期保密培训、签署培训确认书；（4）离岗管控：离职审计、交接清退、保密提醒；（5）监督管控：日常行为审计、异常监测。

法律依据：《商业秘密保护规定》第五条、第九条。

19 涉密信息如何标注密级、限制接触范围？可采取哪些技术防护措施？

答：密级标注与范围限制：（1）强制标注：在涉密文件、图纸、代码、载体上醒目标注密级、保密期限、禁止外传；（2）范围限制：按岗位、职责、必要性设置访问权限，实行“按需知悉”，禁止越权访问。

技术防护措施：（1）加密存储与传输；（2）身份认证、权限管控；（3）水印溯源（文字/屏幕/文件水印）；（4）脱敏处理（隐藏核心参数）；（5）操作日志审计、防拷贝、防截屏、防外发。

法律依据：《商业秘密保护规定》第九条。

20 数字化办公、远程办公场景下，技术保密措施有哪些？

答：（1）边界防护：VPN 安全接入、堡垒机、防火墙、准入控制；（2）终端防护：桌面管控、加密硬盘、防拍摄、防拷贝、禁用私人设备；（3）传输防护：加密传输、脱敏传输、禁止个人社交软件传涉密信息；（4）行为防护：屏幕水印、操作监控、外发审批；（5）审计防护：日志留存、异常报警、行为

追溯。企业应确保数字化办公、远程办公不降低保密标准。

法律依据：《中华人民共和国数据安全法》第二十七条；
《商业秘密保护规定》第九条。

21 涉密文件、代码、设备如何管控？电脑、服务器、云盘、邮箱等如何防泄密？

答：管控手段可以包括：（1）专机专用，涉密电脑禁止联网、禁止外接设备；（2）涉密文件集中存储、统一管理，禁止本地留存；（3）代码纳入代码库，权限分级、提交审核；（4）设备出入库登记、维修报废销毁。

系统防泄密可以包括：（1）服务器：加密、权限、防火墙、日志审计；（2）云盘：禁用私人云盘，企业云盘加密、权限、水印；（3）邮箱：外发审批、脱敏、禁止发送涉密文件；（4）全面禁用 U 盘、私人邮箱、即时通讯传密。

法律依据：《商业秘密保护规定》第九条。

22 保密要求如何嵌入研发流程？研发数据、图纸、模型、仿真文件存储、传输、权限如何有效受控？

答：将保密要求全周期嵌入研发立项、设计、试验、修改、归档、转化全流程，实现研发全程“可管、可控、可追溯”：（1）立项即定密：明确研发成果密级、保护方式；（2）权限受控：按研发角色分级授权，禁止无关人员访问；（3）存储受控：集中加密存储，自动备份、版本留痕；（4）传输受控：加密传输、内部流转、外发审批；（5）使用受控：禁止私自拷贝、截图、外传，操作全程审计；（6）归档受控：研发结束统一归档，纳入涉密载体管理。

法律依据：《商业秘密保护规定》第四条、第九条。

23 企业并购、投融资过程中，如何保护商业秘密？

答：并购、投融资尽调易泄密，需遵循“先保密、后尽调、限范围、留痕迹”原则：（1）协议先行：签订严格的保密协议（NDA），明确约定保密信息的范围、保密期限、使用限制及泄密责任；（2）人员限定：仅允许必要尽调人员接触，签署保密承诺；（3）信息脱敏：提供非核心、脱敏信息，核心秘密非必要不提供；（4）过程管控：现场查阅、禁止拷贝、专人陪同；（5）退出管控：尽调结束返还、销毁涉密资料，签署确认书；（6）证据留存：全程留痕，保存交接、签收记录。

法律依据：《中华人民共和国民法典》第五百零一条；《商业秘密保护规定》第九条、第十二条。

24 境外合作、数据跨境场景下，商业秘密如何保护？

答：境外合作与数据跨境需兼顾国内与境外属地商业秘密法律风险防控：（1）跨境评估：按《数据安全法》完成安全评估，涉及核心数据的需审批；（2）合同约束：与境外合作方签订保密协议，明确属地法律责任；（3）技术保护：加密、脱敏、权限管控，防止境外泄露；（4）范围限制：仅向境外提供必要信息，核心秘密非必要不跨境；（5）属地适配：遵守合作方所在国家/地区商业秘密、数据保护法律；（6）应急机制：建立跨境泄密响应、取证、维权流程。

法律依据：《中华人民共和国数据安全法》第三十一条；《中华人民共和国网络安全法》第四十七条；《中华人民共和国技术进出口管理条例》第二十二条、第四十一条、第四十八条；《商业秘密保护规定》第九条、第二十九条。

25 日常经营中，如何建立并有效执行保密证据留存机制？

答：保密证据留存是维权胜诉的关键，需建立“全流程留痕、分类归档、长期保存”机制：（1）制度类：保密制度发布、签收、公示记录；（2）人员类：保密协议、竞业协议、培训签到、考核记录；（3）技术类：权限设置、操作日志、外发审批、水印记录；（4）载体类：涉密文件收发、借阅、交接、销毁台账；（5）合作类：第三方保密协议、尽调记录、参观登记。电子数据备份、纸质文件归档，保存期限不少于法律诉讼时效。

法律依据：《中华人民共和国民事诉讼法》第六十六条；《商业秘密保护规定》第四条、第九条。

26 如何定期审查保密措施的落实情况？

答：通过定期审计+专项检查+整改闭环，确保保密措施落地：（1）审计频次：每年至少1次全面审计，重大项目、关键岗位专项审计；（2）审计内容：制度执行、人员管理、权限管控、载体管理、技术防护、合作保密、泄密处置；（3）审计方式：自查、第三方审计、现场检查、系统核查、人员访谈；（4）整改闭环：发现问题下达整改通知、限期整改、复查验收、跟踪落实；（5）结果运用：审计结果与绩效考核、奖惩挂钩，强化执行力度。

法律依据：《商业秘密保护规定》第四条、第九条。

27 如何建立合规隔离机制以避免无意中获取或使用未授权信息？

答：综合运用物理隔离、信息隔离、人员隔离三类保密措

施，防范涉密信息的不当获取：（1）物理隔离：涉密区域独立设置、门禁管控、禁止无关人员进入；（2）信息隔离：搭建信息防火墙，涉密系统与非涉密系统分离，禁止跨网访问；（3）人员隔离：涉密人员与非涉密人员分工明确，禁止私自接触竞争对手涉密信息。同时，需细化涉密信息流转规范，禁止贿赂、胁迫、诱导获取他人秘密，并要求员工签署保密承诺，避免过失侵权。

法律依据：《商业秘密保护规定》第九条、第十五条。

28 如何加强技术秘密及科技创新成果专门化管理，完善科技创新成果转化体系及配套制度？

答：围绕“成果确权-保密管理-转化审批-利益分配-风险防控”构建体系：（1）成果清单化：建立科技创新成果台账，明确权属、密级、保护方式；（2）确权清晰：约定职务成果归属，避免权属纠纷；（3）保密并行：转化前严格保密，区分公开转化内容与保密内容；（4）转化审批：对外转化、许可、转让需分级审批，防控泄密；（5）利益分配：明确研发人员奖励、报酬；（6）配套制度：制定成果管理、保密、转化、奖惩制度，实现创新与保密同步。

法律依据：《中华人民共和国促进科技成果转化法》第十一条、第三十条、第四十八条；《商业秘密保护规定》第四条、第五条、第七条、第九条。

（三）落实“合理保密措施”及防止泄露风险

29 如何对入职、在职、离职人员做全流程保密管理？

答：实施“入职-在职-离职”全周期闭环管理：（1）入职环节：审查背景、告知保密义务、签订保密协议、开展入职

保密培训；（2）在职环节：最小权限管控、定期保密培训、日常行为监督、违规预警、考核挂钩；（3）离职环节：清单交接、归还全部涉密载体、注销所有系统权限、签署离职保密承诺、竞业限制提醒、离岗审计。确保人员全流程不泄密、不带密、不滥用秘密。

法律依据：《中华人民共和国劳动合同法》第二十三条；《商业秘密保护规定》第九条。

30 实习生、临时工、劳务派遣人员是否需要签订保密协议？

答：建议签订书面保密协议。实习生、临时工、劳务派遣人员若接触涉密信息，即负有法定保密义务，不因用工形式免除；如未签订协议，难以证明保密措施，维权时举证困难。

法律依据：《中华人民共和国民法典》第五百零一条；《商业秘密保护规定》第九条、第十二条。

31 对第三方劳务派遣、外包等接触保密信息的人员，如何确保保密措施落实？

答：采用“总包负责+合同约束+甲方监管+审计追责+退场清退”模式：（1）总包责任：与派遣/外包公司签订合同，明确其保密管理责任；（2）协议约束：要求第三方人员签订保密协议，约定高额违约责任；（3）甲方管控：限定接触范围、权限、时间，全程陪同监督；（4）审计检查：定期检查第三方保密执行情况，留存记录；（5）退场清退：项目结束收回载体、注销权限、签署无泄密承诺；（6）追责机制：泄密可向第三方与直接责任人双重追责。

法律依据：《民法典》第五百零一条；《商业秘密保护规

定》第九条、第十二条。

32 员工是否需要签订保密协议、竞业限制协议？协议应包括哪些内容？

答：两者适用倾向不同，关于保密协议，所有涉密岗位应该签订，保密义务为法定义务、且一般无固定期限；关于竞业限制协议，则仅适用于高管、高技、核心涉密人员等，企业通常需支付经济补偿，一般附有固定期限。保密协议核心内容一般包括保密范围、期限、涉密载体归还义务、违约责任和争议解决等；竞业限制协议一般包括？人员范围、地域范围、业务范围、期限、经济补偿、违约责任？等核心条款。

法律依据：《中华人民共和国劳动合同法》第二十三条、第二十四条；《商业秘密保护规定》第九条、第十二条。

33 员工离职时的交接流程是什么？曾经接触的技术秘密文件如何处理？

答：离职交接实行“清单化、全收回、全清零、书面确认”标准流程：（1）列出交接清单：列明涉密文件、资料、设备、账号、权限；（2）归还全部载体：纸质文件、硬盘、U 盘、图纸等全部收回，禁止留存；（3）删除电子数据：删除电脑、邮箱、云盘中涉密信息，确认无备份；（4）注销所有权限：注销系统、邮箱、云盘、门禁等权限；（5）签署确认书：员工签署“已全部归还、无涉密信息、继续保密”承诺；（6）全程留痕：交接双方、监交人签字，归档保存。

法律依据：《中华人民共和国劳动合同法》第五十条；《商业秘密保护规定》第九条。

34 针对合作方、外包方、访客，如何落实保密义务？

答：对第三方实行“协议先行、范围限定、过程管控、全程留痕”：（1）合作/外包方：签订正式保密协议，明确保密范围、使用限制、违约责任、审计权；限定接触信息，禁止转委托；定期检查保密执行情况；（2）访客：提前预约、身份登记、签署访客保密承诺；全程专人陪同、禁止进入涉密区域；禁止拍摄、记录、携带电子设备；（3）统一要求：所有第三方均需遵守企业保密制度，违规立即停止合作并追责。

法律依据：《中华人民共和国民法典》第五百零一条；《商业秘密保护规定》第九条、第十二条。

35 对签有竞业限制协议的离职人员，如何合法有效调查其是否入职竞争对手？

答：调查需严格合法，禁止侵犯个人信息、隐私，合法方式包括：（1）公开信息核查：企业公示信息、官网、招聘信息、新闻报道等；（2）社保/个税查询：通过合法渠道核实缴纳单位；（3）实地核实：公开场所、办公地点外观观察；（4）自愿核实：向员工本人、原同事合法询问；（5）委托第三方机构：委托律师、征信机构合法调查。禁止非法获取通话记录、定位、开房记录、聊天记录等隐私信息。

法律依据：《中华人民共和国劳动合同法》第二十四条；《中华人民共和国个人信息保护法》；《商业秘密保护规定》第十二条。

36 对外展示、参观、交流时，如何避免泄露技术秘密？

答：遵循“预审、脱敏、屏蔽、陪同、禁拍”五步法：（1）内容预审：展示、交流材料提前涉密审查，删除核心秘

密；（2）信息脱敏：隐藏配方、参数、工艺、核心结构；（3）区域屏蔽：封闭涉密车间、实验室、研发室，禁止参观；（4）全程陪同：专人陪同参观，控制路线、时间；（5）禁止拍摄：张贴禁拍标识，禁止记录；（6）口头限制：禁止讲解核心技术、未公开信息。

法律依据：《商业秘密保护规定》第九条。

37 委托开发、测试、生产时，如何控制技术扩散？

答：委托合作需严控技术扩散，缩小知情范围：（1）合同约束：明确保密义务、技术使用范围、知识产权归属、禁止转委托；（2）技术拆分：拆分技术环节，仅提供必要部分，核心技术自留；（3）信息脱敏：提供非核心、加密、脱敏技术资料；（4）人员限定：仅允许受托方指定人员接触，签署保密承诺；（5）过程监督：现场监督、定期检查、禁止私自留存技术资料；（6）成果回收：合作结束收回全部技术资料、样品，销毁备份。

法律依据：《中华人民共和国民法典》第八百六十一条；《商业秘密保护规定》第九条、第十二条。

38 展会、论文、专利申请中，如何避免无意中公开秘密？

答：公开场景易发生泄密，需严格前置审查：（1）展会：展品、资料预审，核心参数不展示、不讲解；（2）论文：发表前涉密审查，删除未公开技术秘密、数据、配方；（3）专利申请：合理布局，规避核心秘密，仅公开必要技术特征，核心内容作为技术秘密保留；（4）统一要求：所有对外公开内容，须经内部保密审查，确认不丧失秘密性后方可发布。

法律依据：《商业秘密保护规定》第五条、第六条。

39 涉密文件对外发送、合作共享有哪些风控要点？

答：对外发送、共享需分级审批、最小供给、全程留痕：

- (1) 审批管控：高密级文件高层审批，低密级部门审批；
- (2) 脱敏管控：隐藏核心数据、参数、配方，仅提供必要内容；
- (3) 加密管控：加密发送、设置阅读权限、有效期、禁止下载；
- (4) 渠道管控：使用企业指定加密渠道，禁止使用个人社交软件、私人邮箱发送工作文档；
- (5) 责任管控：约定接收方保密义务、禁止转发、泄密追责；
- (6) 留痕管控：保存发送记录、签收记录、阅读记录。

法律依据：《商业秘密保护规定》第九条。

40 外聘专家、合作研发、联合开发、高校合作的保密要求有哪些关键点？

答：外部研发合作核心是确权 + 保密 + 限用：(1) 签订保密协议：所有合作方、专家均需签署，明确保密义务；(2) 明确权属：约定技术成果、秘密归属，避免纠纷；(3) 使用限制：仅限合作项目使用，禁止擅自使用、披露、发表；(4) 发表审查：论文、著作、成果发布需企业预审，禁止公开秘密；(5) 人员管理：限定接触人员，禁止扩散给第三方；(6) 成果管理：合作结束收回技术资料，保密义务持续有效。

法律依据：《中华人民共和国民法典》第八百四十五条、第八百四十六条、第八百六十一条；《商业秘密保护规定》第九条、第十二条、第十五条。

41 与供应商、外包方合作时，除保密协议外，有哪些检查或审计方法核实其履行保密义务？

答：可通过多种审计或检查方式监督第三方履约，确保保

密落实：(1) 现场审计：实地检查涉密载体管理、人员执行、设备安全；(2) 系统审计：核查其信息系统权限、日志、存储、外发记录；(3) 人员访谈：访谈接触秘密的人员，了解执行情况；(4) 资料核查：检查其保密制度、培训记录、台账；(5) 定期汇报：要求供应商定期提交保密执行报告；(6) 突击检查：必要时突击抽查，防范违规。合同中需明确企业享有审计权。为保障相关措施顺利实施，在合作协议中应事先明确约定企业可以实施前述审计或检查措施。

法律依据：《民法典》第五百零一条；《商业秘密保护规定》第九条、第十二条。

42 对外合作（如委托加工）中，如何防范合作方通过反向工程获取核心技术秘密？

答：反向工程是合法获取手段，需从技术、合同、管理上提前阻断：(1) 技术拆分：仅提供加工所需局部信息，不提供完整技术方案；(2) 合同禁止：明确约定禁止反向工程、拆解、分析、仿制；(3) 核心自留：核心配方、工艺、组装工序由企业自行完成；(4) 信息脱敏：提供加工数据时隐藏核心参数；(5) 过程管控：现场监督加工，禁止私自留存样品、废料；(6) 技术保护：对核心技术加密、模糊化处理，增加反向工程难度。

法律依据：《商业秘密保护规定》第九条、第十二条、第十五条。

43 使用开源代码，如何避免污染自有商业秘密？

答：使用开源代码时，需注意合规使用和物理隔离，防止商业秘密被开源“污染”：(1) 协议审查：严格审查开源协

议，明确传播、修改、闭源要求；（2）物理隔离：开源代码与自有商业秘密代码分开存储、分开开发、分开部署，禁止混合编写；（3）边界清晰：不将商业秘密写入开源模块，不修改开源代码后纳入秘密代码；（4）证据留存：留存开源来源、协议、使用记录；（5）风险自查：定期检查代码来源合法性，避免侵权与泄密。

法律依据：《中华人民共和国民法典》第一百二十三条；《商业秘密保护规定》第四条。

44 如何有效避免离职研发人员带走方案、参数、文档的风险？

答：构建“事前-事中-事后”全链条防控体系，从技术、管理、法律方面多重防范：（1）事前：权限最小化，禁止私自下载、拷贝、截图、外传；（2）事中：技术监控（水印、日志、告警），实时发现异常；（3）离职：全面清退设备、账号、载体，签署“不带走、不使用、不披露”承诺；（4）事后：违约追责，要求返还、停止使用、赔偿损失。

法律依据：《中华人民共和国劳动合同法》第二十三条、第五十条；《商业秘密保护规定》第九条、第十二条。

45 如何加强科技创新成果技术信息安全管控，健全技术秘密载体管理？

答：技术秘密载体实行“台账化、集中化、授权化、全生命周期”管理：（1）台账管理：建立载体台账，记录编号、密级、内容、责任人、存放位置；（2）集中存储：纸质载体入保密柜，电子载体入加密服务器/云盘；（3）授权使用：借阅、复制、传输需审批，全程留痕；（4）流转管控：内部流转签字

确认，外部流转加密审批；（5）销毁管控：报废载体粉碎、删除，签署销毁记录；（6）安全管控：防盗、防火、防潮、防篡改、防泄露。

法律依据：《商业秘密保护规定》第四条、第九条。

46 如果被诉侵权，如何以合法来源进行抗辩？

答：合法来源抗辩是法定免责/减责事由，需同时满足四个要件：（1）信息来源合法：通过合法受让、许可、合作、自行研发、合法反向工程获取；（2）支付合理对价：有偿获取，非无偿、非窃取；（3）主观善意：不知且不应知信息是他人商业秘密；（4）尽到合理注意义务：审查权属、协议、来源证明。

法律依据：《中华人民共和国反不正当竞争法》第十条、第三十六条；《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》第十四条；《商业秘密保护规定》第十五条。

（四）侵犯商业秘密行为认定

47 法律规定的侵犯商业秘密行为有哪些典型类型？电子侵入、云端窃密是否属于侵权？

答：法定侵权类型：（1）不正当获取：盗窃、贿赂、欺诈、胁迫、电子侵入等；（2）非法使用披露：使用、允许他人使用非法获取的秘密；（3）违反义务披露：违反保密协议/要求，披露、使用秘密；（4）教唆帮助侵权：教唆、引诱、帮助他人侵权；（5）恶意第三人侵权：明知/应知侵权，仍获取、使用、披露。电子侵入、云端窃密明确属于侵权，是法律重点规制的数字化侵权行为。

法律依据：《商业秘密保护规定》第十条至第十四条。

48 未签订书面保密协议，是否负有商业秘密保密义务？

答：未签订书面协议，行为人知道或者应当知道其获取的信息属于权利人商业秘密的，仍可认定行为人对其获取的信息承担保密义务。基于劳动关系、委托关系、合作关系、诚实信用原则，接触商业秘密的人员均需保密；即便无书面协议，也构成默示保密义务。司法、行政机关认可默示保密义务，不以书面协议为唯一依据；书面协议仅为强化证据，无协议不代表无义务，仍可认定侵权。但在未签订书面保密协议的情况下，企业主张商业秘密保护时的举证责任较重，建议企业签署书面保密协议。

法律依据：《中华人民共和国民法典》第五百零一条、第五百零九条；《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》第十条；《商业秘密保护规定》第十二条。

49 如何证明“技术秘密一旦泄露会造成损失”？

答：证明泄露会造成损失，是认定价值性与侵权后果的关键，可通过以下证据证明：（1）研发成本：投入的人力、物力、财力、时间成本；（2）市场价值：产品售价、利润、市场份额、竞争优势；（3）许可价值：技术许可使用费、转让费；（4）竞争影响：泄露后导致客户流失、报价透明、优势丧失；（5）专家意见：行业专家出具损失评估意见。

法律依据：《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》第十九条；《商业秘密保护规定》第十五条。

50 侵犯商业秘密的举证责任如何分配？企业举证难怎么办？

答：举证责任分配：（1）权利人初步举证：证明拥有商业秘密、对方接触过秘密、双方信息实质性相同；（2）举证责任转移：由侵权方证明信息来源合法、未侵权。举证难解决路径：（1）证据保全：向法院申请诉前/诉中证据保全；（2）调查令：申请律师调查令调取证据；（3）司法鉴定：委托鉴定信息同一性、秘密性；（4）公证取证：对侵权信息公证固定。

法律依据：《中华人民共和国民事诉讼法》第六十七条、第八十四条；《中华人民共和国反不正当竞争法》第三十九条；《商业秘密保护规定》第十七条、第十八条、第二十条。

51 合作开发、委托开发中的技术秘密归属如何确定？

答：技术秘密归属“有约定从约定，无约定依法定”：（1）委托开发：有约定按约定；无约定的，技术秘密归受托人（研发方），委托人享有免费使用权；（2）合作开发：有约定按约定；无约定的，归合作各方共有，一方转让需其他方同意，一方放弃可由其他方共有，放弃方享有免费使用权。

法律依据：《中华人民共和国民法典》第八百五十九条、第八百六十条。

52 并购、投资、合作时，如何界定原有秘密与新增秘密？

答：可以时间节点、权属来源、研发贡献清晰界定：（1）原有秘密：并购/投资/合作前，一方已拥有的商业秘密，归原权利人所有；界定依据：交接清单、研发记录、申请文

件、保密台账、时间戳等；(2) 新增秘密：合作后共同研发、改进形成的新秘密，按合同约定归属；无约定按合作开发共有；(3) 区分管理：分别建档、分别授权、分别保护，避免权属混同、侵权纠纷。

法律依据：《中华人民共和国民法典》第五百零一条、第八百四十五条、第八百六十条；《商业秘密保护规定》第十二条、第十五条。

53 侵犯商业秘密情节严重的认定标准是什么？

答：“情节严重”由司法、行政机关综合多因素认定，核心标准：(1) 金额标准：侵权获利大、权利人损失高；(2) 手段标准：采取电子侵入、盗窃、胁迫、团伙作案等恶劣手段；(3) 范围标准：泄露范围广、传播速度快、影响行业竞争；(4) 后果标准：导致企业停产、亏损、破产、丧失核心竞争力；(5) 主观标准：恶意明显、多次侵权、拒不停止侵权；(6) 其他标准：涉及核心技术、国家重要产业、公共利益。

法律依据：《中华人民共和国反不正当竞争法》第二十六条；《商业秘密保护规定》第二十六条。

54 商业秘密民事侵权、行政违法、刑事犯罪的界限是什么？

答：三者按行为性质、后果严重程度层层递进：(1) 民事侵权：存在侵权行为，造成损失/获利，承担赔偿责任、停止侵害、赔礼道歉等民事责任；(2) 行政违法：侵权行为违反监管规定，由市场监管部门责令停止违法行为、没收违法所得、罚款；(3) 刑事犯罪：侵权行为情节严重，构成侵犯商业秘密罪的，依法承担有期徒刑、并处或单处罚金等刑事责任。

法律依据：《中华人民共和国反不正当竞争法》第二十六条；《中华人民共和国刑法》第二百一十九条；《商业秘密保护规定》第二十六条。

55 哪些行为属于侵犯商业秘密的免责情形？

答：以下行为合法，不构成侵权，属于法定免责：（1）自行研发：独立研发、构思出相同信息；（2）合法反向工程：对公开产品拆解、分析、测绘获得信息；（3）合法受让/许可：通过转让、许可合法取得；（4）权利人公开：权利人主动公开、默示允许使用；（5）法定披露：司法、行政程序中依法披露；（6）公共利益披露：为维护公共利益合法披露。免责需证明行为合法、主观善意。

法律依据：《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》第十四条；《商业秘密保护规定》第十五条。

56 员工违反保密义务，企业能否直接开除并追责？

答：员工严重违反保密义务，符合下列情形的，企业可依法解除劳动合同并追责：员工存在泄露、使用、非法披露秘密等严重违反义务行为，且依据企业规章制度此等情形可导致解除劳动合同。

法律依据：《中华人民共和国劳动合同法》第三十九条。

57 商业秘密被泄露后，如何固定电子证据？

答：电子证据易篡改，需合法、规范、完整固定：（1）公证保全：申请公证处对网页、聊天记录、文件、邮件公证；（2）司法鉴定：委托司法鉴定机构固定、提取、校验电子数

据；(3) 原始留存：保存原始设备、原始文件、原始日志，不删除、不修改；(4) 哈希校验：计算文件哈希值，证明未篡改；(5) 截图录屏：对侵权页面、传播记录完整录屏、截图；(6) 日志导出：导出系统日志、操作日志、访问日志。

法律依据：《中华人民共和国民事诉讼法》第六十六条；《商业秘密保护规定》第十七条、第十八条。

58 员工泄露未在制度中明确列举的保密信息，如何证明该信息属于保密信息？如何证明泄密损失或对方获利？

答：即便制度中未列举，企业仍可按三要件举证证明：秘密性（非公知）、价值性（有优势）、保密性（企业采取措施，员工知晓保密）。

证明损失/获利：（1）研发成本、利润减少、许可费、维权合理开支；（2）侵权方销量、利润、节省的研发成本；（3）无法计算时，主张法定赔偿。

法律依据：《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》第十九条；《商业秘密保护规定》第六条、第七条、第九条。

59 员工离职后，哪些知识经验属合法可使用的自身技能？哪些属不能随意披露使用的商业秘密？

答：可合法使用的个人技能：行业常识、通用专业知识、基础操作技能、个人职业经验、公知信息，属于个人积累，可自由使用；禁止使用披露的商业秘密：企业非公知、有价值、已保密的技术方案、配方、工艺、客户名单、报价、数据等，属于企业资产，离职后仍需保密，擅自使用、披露构成侵权。

法律依据：《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》第四条；《商业秘密保护规定》第十四条、第十五条。

60 员工离职后入职竞品并使用原单位技术信息是否一定构成侵权？

答：不一定构成侵权，需区分使用内容。不侵权：使用个人通用技能、行业常识、公知信息，未使用原单位商业秘密；构成侵权：使用原单位符合三要件的商业秘密，且违反保密义务、竞业限制义务。司法实践中，法院会对比信息内容，区分“个人技能”与“商业秘密”，仅使用秘密信息才认定侵权。

法律依据：《商业秘密保护规定》第十四条、第十五条。

61 核心研发员工离职后，能否以“成果含个人核心技能”为由在竞品处继续使用原履职期间主导的技术？

答：首先，员工履职期间形成的技术成果，可能属于职务技术成果，权利归企业所有，并非个人所有；其次，如果该技术符合商业秘密三要件，则受法律保护，员工负有法定或约定保密义务，禁止使用、披露。个人技能不能当然成为使用企业商业秘密的合法理由，需根据具体情形具体分析。

法律依据：《中华人民共和国民法典》第一百二十三条；《商业秘密保护规定》第十四条。

62 商业秘密被泄露但尚未造成实际损失，能否主张赔偿以及损失如何计算？

答：即便尚未发生直观的经济损失，权利人仍有权主张赔偿并要求停止侵害。第一，商业秘密的核心价值在于秘密性，一旦泄露即导致价值贬损、竞争优势削弱，法律保护不以“

实际损失已发生"为前提；第二，损失可按照合理许可使用费标准计算，即参照该秘密通常可获得的许可费用确定赔偿额；第三，侵权人因此获得的利益、权利人为维权支出的合理费用（公证费、鉴定费、律师费等）均可纳入赔偿范围；第四，恶意侵权、情节严重的，可依法主张惩罚性赔偿。未造成实际经济损失，不影响侵权认定与责任承担。

法律依据：《中华人民共和国反不正当竞争法》第二十二条；《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》第十九条。

63 境外形成的商业秘密，在我国境内能否获得保护？

答：境外形成的商业秘密，在我国境内可以依法获得保护，前提是该信息需符合我国法律规定的秘密性、价值性、保密性三要件。权利人需提供合法权属证明、保密措施证据、侵权证据，境外形成不影响境内保护，保护标准与境内形成的商业秘密一致。

法律依据：《商业秘密保护规定》第五条、第二十九条。

（五）商业秘密保护途径与维权措施

64 商业秘密疑似泄露或被侵权，应启动哪些紧急应对流程？

答：泄密后必须快速响应、闭环处置，按以下步骤执行：
（1）紧急止损：立即切断泄露渠道，收回涉密载体，关停权限，删除泄露信息，防止扩散；（2）固定证据：对网页、文件、聊天记录、日志、设备等进行公证、录屏、哈希校验，防止证据灭失；（3）内部核查：排查泄露时间、渠道、人员、范围，形成调查报告；（4）交涉停止：向侵权方发送律师函/

停止侵权函，要求立即停止获取、使用、披露；（5）法律措施启动：根据情节轻重，选择申请证据保全、提起民事诉讼、向市监部门举报或向公安机关刑事报案；（6）复盘加固：修补保密漏洞，升级管控措施，避免再次泄密。

法律依据：《中华人民共和国反不正当竞争法》第二十六条；《中华人民共和国刑法》第二百一十九条；《中华人民共和国民事诉讼法》第一百二十二条。

65 企业如何主动监测商业秘密被侵犯，是否有成熟监测机构或技术手段？

答：企业可构建技术监测 + 人工核查 + 第三方服务的立体监测体系：（1）技术手段：数据防泄漏系统、文件水印溯源、操作行为审计、外发流量监测、云端异常访问告警；（2）人工手段：定期检索竞品产品、宣传资料、招聘信息、专利申请，比对是否使用本企业秘密。可委托律师事务所、商业调查机构、知识产权服务机构、司法鉴定机构开展监测、调查、取证；监测重点是核心数据外发、离职人员流向、竞品技术突变、公开渠道披露、异常文件访问等。

法律依据：《商业秘密保护规定》第十七条、第十九条、第二十二条。

66 商业秘密维权有哪些途径？刑事报案、行政举报、民事诉讼的优劣势及适用条件是什么？

答：商业秘密维权有民事、行政、刑事三条路径，可根据具体情形选择推进路径。

民事诉讼：优势为可主张全面赔偿、停止侵害、消除影响；劣势为周期较长、举证要求高；适用于追求经济赔偿、民

事责任追究。

行政举报（向市场监管部门）：优势为程序较快、成本低、调查力度强、可快速制止侵权；劣势为无民事赔偿；适用于快速制止侵权、获取调查证据、施加行政压力。

刑事报案：优势为打击力度最强、调查取证能力最强、震慑效果最大；劣势为立案标准高、需达到“重大损失”；适用于侵权情节恶劣、造成重大损失、涉嫌侵犯商业秘密罪。

法律依据：《中华人民共和国反不正当竞争法》第二十六条；《中华人民共和国刑法》第二百一十九条；《中华人民共和国民事诉讼法》第一百二十二条。

67 提起商业秘密民事诉讼，管辖法院如何确定？

答：地域管辖：由侵权行为地（包括侵权实施地、侵权结果发生地）或者被告住所地人民法院管辖；级别管辖：一般由中级以上人民法院管辖，部分基层法院经最高院批准可管辖。企业可优先选择司法保护力度强、审理专业度高的法院。

法律依据：《中华人民共和国民事诉讼法》第二十九条。

68 民事维权中可主张哪些赔偿？赔偿数额/损失/违法所得如何计算？

答：因商业秘密被侵犯受到损害的经营者的赔偿数额，按照权利人因被侵权所受到的实际损失或者侵权人因侵权所获得的利益确定。经营者故意实施侵犯商业秘密行为，情节严重的，可以在按照上述方法确定数额的一倍以上五倍以下确定赔偿数额。赔偿数额还应当包括经营者为制止侵权行为所支付的合理开支。权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益难以确定的，由人民法院根据侵权行为的情节判

决给予权利人五百万元以下的赔偿。

法律依据：《中华人民共和国反不正当竞争法》第二十二
条、第二十六条。

69 向市场监管部门投诉侵犯商业秘密，需准备哪些材料？行政投诉处理流程和时限是多久？

答：投诉必备材料：（1）投诉书（明确请求、事实、理由）；（2）权利人主体资格证明；（3）商业秘密权属及三要件证明（秘密性、价值性、保密性）；（4）侵权行为证据（获取、使用、披露行为）；（5）损失或获利证据；（6）证据清单、来源说明。处理流程：受理→立案→调查取证→审理→处罚决定→执行。办理时限：一般自立案之日起 90 日内作出处理决定；情况复杂可依法延长。

法律依据：《商业秘密保护规定》第十七条、第十八条、第十九条。

70 如何证明对方“获取、使用、披露”了企业的技术秘密？

答：证明对方实施侵权行为，需构建接触+实质性相同+无合法来源的证据链。证明接触：对方曾在我方任职、合作、参观、尽调，有条件接触秘密；证明实质性相同：对方产品、技术、文件、配方、工艺与我方秘密构成实质性相同，可通过司法鉴定确认；证明获取/使用/披露：公开宣传资料、产品拆解、销售资料、论文、专利申请、员工证言、电子数据、公证录像等；排除合法来源：对方无法证明自行研发、合法受让、反向工程等合法来源。

法律依据：《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》第十一条；《商业秘密保护规定》第二十条。

71 维权中法院或行政主管部门最认可的证据类型有哪些？如何确保证据合法、真实、关联？

答：高证明力证据：公证文书、司法鉴定意见、保密协议、制度签收记录、电子存证、权限日志、银行/税务数据、官方公示信息。合法性：取证手段合法，不偷拍偷录、不侵入系统、不获取隐私，委托公证/律师取证；真实性：原始载体留存、电子数据哈希校验、时间戳固定、不剪辑不修改；关联性：证据直接指向商业秘密本身、侵权行为、损失后果，与案件事实相关。证据越规范、越原始、越中立，采信度越高。

法律依据：《中华人民共和国民事诉讼法》第六十六条、七十三条；《最高人民法院关于民事诉讼证据的若干规定》第十四条、第十五条、第九十三条。

72 哪些情形下侵犯商业秘密会构成刑事犯罪？

答：采取不正当手段，获取、使用、披露或者允许他人使用权利人的商业秘密，给商业秘密的权利人造成重大损失的，构成侵犯商业秘密罪。行为类型：以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密的；披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；违反约定或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。

法律依据：《中华人民共和国刑法》第二百一十九条。

73 企业可获得哪些商业秘密保护公共服务支持？

答：企业可免费或低成本获得官方公共服务：（1）政策指导：市场监管部门等政府主管部门提供商业秘密保护指引、制度模板、培训宣讲；（2）知识产权公共服务：知识产权保护中心、维权援助中心提供咨询、调解、援助；（3）法律服务：法律援助机构、律师公益服务提供法律意见；（4）专业服务：公证处、司法鉴定机构提供规范取证、鉴定服务；（5）纠纷调解：行政调解、行业调解、人民调解快速化解纠纷，降低成本。

法律依据：《商业秘密保护规定》第四条、第二十二条。

74 商业秘密与国家秘密重合时如何保护？

答：当商业信息属于国家秘密时，按照国家秘密保护，执行《保守国家秘密法》规定，严格定密、管控。

法律依据：《中华人民共和国保守国家秘密法》第二条、第十条；《商业秘密保护规定》第二十八条。

75 维权过程中，如何防止商业秘密二次泄露？

答：维权举证极易导致二次泄密，须采取保密诉讼措施：（1）申请不公开审理，禁止旁听；（2）证据保密质证，仅法官、对方律师（签署保密承诺）可查阅；（3）裁判文书隐名处理，申请不公开文书或隐去秘密内容；（4）证据材料分级管控，标注密级、限制复制、限制传播。

法律依据：《中华人民共和国民事诉讼法》第一百三十七条、第一百三十九条；《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》第二十六条。

76 如何避免因自身保密措施不足导致败诉？

答：保密措施不足是维权不成功的主要原因之一。企业须做到：（1）制度完备：有正式保密制度、秘密清单、密级划分并公示签收；（2）协议齐全：涉密人员、第三方均签保密协议；（3）管理落地：涉密载体、设备、区域、权限有管控、有记录；（4）措施合理：采取与秘密价值匹配的保密手段，不流于形式；（5）证据留存：制度、培训、权限、交接、审计全程留痕；（6）定期审计：持续检查、整改、优化。

法律依据：《商业秘密保护规定》第五条、第六条、第九条。

77 海外子公司（工厂）是否需要建立符合当地法规的商业秘密保护制度？

答：需要建立，且实行双重合规：（1）遵守我国《反不正当竞争法》、《数据安全法》和《商业秘密保护规定》等相关法律法规；（2）严格遵守东道国商业秘密、数据保护、劳动用工、知识产权等相关法律法规；（3）制度本地化：结合当地用工习惯、数据合规、证据规则设计；（4）跨境管控：统一保密标准，分级授权，跨境数据合规；（5）风险应对：建立海外泄密应急、当地维权、跨境取证机制。

法律依据：《中华人民共和国数据安全法》第三十一条；《商业秘密保护规定》第二十九条。

78 招录竞品离职员工，如何设计人事合规制度防范“共同侵权”及单位犯罪风险？

答：企业招录竞争对手离职员工时，极易因不当使用前雇主商业秘密构成共同侵权甚至单位犯罪，须建立全流程合规防

火墙：(1) 入职前尽职审查：主动询问并书面核实员工与前单位是否存在保密协议、竞业限制协议；要求员工签署《无竞业限制/无侵权承诺函》，承诺未携带、未使用、未披露前单位商业秘密；对核心岗位员工开展背景调查，确认无侵权风险。(2) 入职时强制隔离：明确告知并书面要求不得带入、不得使用、不得存储前单位任何涉密资料、文件、数据、设备、代码、图纸、客户信息；签署《信息隔离与保密合规承诺书》，将禁止行为写入规章制度。(3) 入职后物理与技术隔离：新员工设备统一配发、清空处理，严禁使用私人设备或前单位遗留设备；建立独立项目组、独立账号、独立权限，与现有技术信息区隔；禁止新员工接触与前单位业务高度重合的核心项目、涉密信息。(4) 培训与留痕：开展商业秘密合规培训，明确侵权后果与法律责任；全程留存承诺函、协议、培训记录、签到记录、设备交接记录。(5) 违规追责机制：员工隐瞒竞业限制、私自使用秘密的，企业可立即解除合同并追责；企业自身不教唆、不诱导、不鼓励员工使用前单位秘密，杜绝主观过错。通过上述制度，可最大限度降低共同侵权、行政处罚、刑事追责风险。

法律依据：《商业秘密保护规定》第十四条、第十五条。

79 如何建立海外泄密应急预案、跨境响应机制？

答：海外泄密因地域、法律、语言、证据规则差异，处置难度更高，须建立标准化、可落地、跨境协同的应急预案。建立分级响应机制：一级泄密为核心技术/核心经营信息泄露，立即启动最高级响应；二级泄密为局部信息泄露，限定范围处置；三级泄密为疑似泄露、风险预警，开展核查。明确跨境组织架构：设立境内总指挥（法务/高管）+ 海外属地责任人（子公司负责人/合规官）+ 当地律师 + 公关负责人；明确联

络流程、权限、决策路径。跨境证据固定规则：委托当地公证、律师、调查机构取证，符合当地证据标准；同步进行电子数据存证、哈希校验、日志留存；确保跨境证据可在境内外司法程序中使用。属地化法律应对：按当地法律发送停止侵权函、申请禁令、提起诉讼或行政举报；同步在我国境内启动维权，实现境内外双线追责。复盘与改进：事件结束后形成跨境泄密报告，优化制度、权限、技术、流程；定期开展海外泄密应急演练。

法律依据：《中华人民共和国数据安全法》第三十一条；《商业秘密保护规定》第二十九条。

80 商业秘密侵权纠纷中，当事人双方能否通过调解方式解决？调解协议具有怎样的法律效力？

答：商业秘密侵权纠纷可以通过调解方式高效、保密解决。可向人民法院、市场监管部门申请调解，也可由知识产权保护中心、行业协会、人民调解委员会等第三方机构主持调解。经调解达成的协议具有民事合同约束力，一方不履行的另一方可提起诉讼；经法院司法确认后的调解协议，具有强制执行力，可直接申请法院强制执行。

法律依据：《中华人民共和国人民调解法》第三十一条、第三十二条、第三十三条。

三、商业秘密保护典型案例集

（一）商业秘密界定相关案例

案例 1 技术信息符合三性，认定为技术秘密

案号：（2022）最高法知民终 719 号

审理法院：最高人民法院

要点及案例分析：

技术秘密与专利虽同为知识产权，但技术秘密保护与专利权保护并不相同，技术秘密的法律保护并无新颖性、创造性等要求，只要其符合法定的秘密性、价值性、保密性即可。即便图纸的部分技术信息已经存在于公共领域，如果信息持有人对公开信息进行了整理、改进、加工以及组合、汇编而产生新信息，他人不经一定努力无法轻易获得，该新信息经采取保密措施同样可以成为技术秘密而受到法律保护。不宜要求商业秘密权利人对其所主张的技术秘密与公知信息的区别作过于严苛的证明。权利人提供了证明技术信息秘密性的初步证据，或对其主张的技术秘密之“不为公众所知悉”做出合理的解释或说明，即可初步认定秘密性成立；如果同时证明相关技术信息具备价值，并采取了保密措施，可以作为技术秘密予以保护。

案例 2 信息仅含公知内容，不构成商业秘密

案号：（2021）最高法民再 310 号

审理法院：最高人民法院

要点及案例分析：

原告仅提交客户名称、电话、地址等可公开查询的信息，未包含交易习惯、合作底价、深度需求等非公知内容，不具备秘密性与价值性；未采取针对性保密措施，不满足保密性要求。因此，仅包含公知信息且未采取保密措施的客户资料，不构成商业秘密。

案例 3 业务客户已知晓信息，不必然否定商业秘密成立

案号：（2022）最高法知民终 26 号

审理法院：最高人民法院

要点及案例分析：

权利人主张的经营信息包含客户名称、代码、联系人、需求、交易情况等深度内容，并非简单公开信息。商业秘密具有相对性，客户知晓交易价格不代表行业内普遍知悉，且权利人已与客户签订保密协议，客户负有保密义务，涉案经营信息符合三性要求，构成商业秘密。

（二）管理保护体系建设相关案例

案例 4 保密体系完善，维权请求获法院支持

案号：（2019）最高法知民终 562 号

审理法院：最高人民法院

要点及案例分析：

权利人通过签订《劳动合同》、《专项保密协议》、《商业秘密/竞业限制协议》等方式，对技术信息保密做出明确约定，已采取多样化保密措施，符合司法解释关于“合理保密措施”的认定标准。结合技术信息特性、权利人保密意愿、保密措施可识别程度、他人正当获取难易程度等因素，认定权利人已采取合理保密措施，商业秘密依法受保护。

案例 5 未落实有效保密措施，商业秘密主张不成立

案号：（2020）最高法知民终 538 号

审理法院：最高人民法院

要点及案例分析：

技术秘密载体为市场流通产品的，权利人内部保密措施不

能对抗不特定第三人，需采取可对抗反向工程的外部保密措施。权利人仅在产品上贴附保密标签、单方禁止拆解，无法对抗他人合法所有权，不属于反不正当竞争法规定的“相应保密措施”，商业秘密主张不能成立。

（三）制度落实与日常风控相关案例

案例 6 离职员工违反保密义务泄密，企业追责成功

案号：（2022）最高法知民终 147 号

审理法院：最高人民法院

要点及案例分析：

权利人与离职员工签订保密协议，员工离职时完成涉密载体交接、权限注销后，仍负有法定及约定保密义务。员工离职后将技术秘密披露给竞争公司，违反保密义务构成侵权；竞争公司明知技术信息系员工违反保密义务披露仍予以使用，属于法律规定的“明知或应知违法获取仍使用”情形，应与员工承担连带赔偿责任。

案例 7 受让技术未尽审慎注意义务，构成商业秘密侵权

案号：（2022）最高法知民终 901 号

审理法院：最高人民法院

要点及案例分析：

被告在受让涉案软件时，未对核心数据库来源合法性尽到足够审慎注意义务：明知数据库体量大、研发周期短，未核查转让人研发能力与数据来源；未核实转让人履历与权利人的关联关系；对转让人履历矛盾、社保缴纳异常等情形未进一步查证。被告未尽审慎注意义务，受让并使用与权利人技术秘密实质相同的信息，构成侵害商业秘密，应承担侵权责任。

（四）侵权行为及赔偿认定相关案例

案例 8 涉密员工集中离职并入职新公司，引发侵权纠纷的风险高

案号：（2023）最高法知民终 1590 号

审理法院：最高人民法院

要点及案例分析：

被告通过招聘原告关联公司近 40 名离职技术人员（均接触原告涉案技术秘密），短时间内实现电动汽车量产。对于此种以多名曾接触或者掌握涉案技术秘密的员工短时间内集中从原单位离职并入职新公司为表现形式的有组织、有计划的行为，如果被诉侵权人即新公司在明显短于独立研发所需合理时间内即生产出与涉案技术秘密相关的产品，而被诉侵权人有渠道或者机会获取涉案技术秘密，此时因侵权可能性极大，应当进一步减轻技术秘密权利人对于侵害技术秘密行为的证明负担。此时，可以直接推定被诉侵权人实施了侵害权利人技术秘密的行为。被诉侵权人否认其实施侵害技术秘密行为的，应当提供证据予以反驳，否则，一般应认定被诉侵权人构成侵害技术秘密。

案例 9 通过合法反向工程获取信息，不构成侵权

案号：（2021）最高法知民终 1440 号

审理法院：最高人民法院

要点及案例分析：

被告通过合法渠道购买权利人公开销售的产品，以公众均可实施的方式拆解观测，使用常规工具测量无法直接观察的参数与连接关系，未采取盗窃、贿赂、电子侵入等不正当手段，亦未违反保密义务，属于合法反向工程，不构成侵害商业秘密。

案例 10 “接触”要件举证不足，侵权追责未获支持

案号：(2023) 最高法知民终 2587 号

审理法院：最高人民法院

要点及案例分析：

现有证据仅证明被告参与前期调研等活动，与技术秘密研发、测试无直接关联，无法证明被告实质性接触涉案技术秘密。权利人主张被告可通过调研、采购接触秘密，但缺乏证据佐证；若仅凭上述活动即可获取秘密，反而证明权利人未采取合理有效保密措施，涉案信息不应获得保护。

案例 11 参考事前保密约定金额，确定侵害技术秘密赔偿额

案号：(2021) 最高法知民终 1687 号

审理法院：最高人民法院

要点及案例分析：

原告与被告在《保密协议书》中明确约定数据库、源代码等为绝密信息，原告按月支付被告保密工资，并约定违反保密义务赔偿 50—100 万元。该约定属于侵权损害赔偿事前约定，法院确定赔偿数额时可作为重要参考。法院综合技术秘密研发成本、侵权人主观恶意、仅窃取未扩散使用等情节，在约定区间内酌定赔偿 25 万元，并支持维权合理开支 1.5 万元。

案例 12 综合考量多项因素，全额支持原告赔偿诉请

案号：(2023) 最高法知民终 120 号

审理法院：最高人民法院知识产权法庭

要点及案例分析：

法院确定赔偿数额时重点考量四项因素：1. 涉案技术秘

密属于医用制氧领域，应用广泛、市场需求大，商业价值较高；2. 侵权人系权利人前高管，在职设立同业公司，曾因侵权调解结案后仍重复侵权，主观恶意明显；3. 侵权行为持续多年，中标多个医院采购项目，侵权情节严重；4. 侵权人无正当理由拒不提交财务账簿，构成举证妨碍，应承担不利后果。综合上述因素，法院全额支持权利人 500 万元赔偿主张。

案例 13 主观恶意明显，可适用惩罚性赔偿及迟延履行金

案号：（2022）最高法知民终 1592 号

审理法院：最高人民法院

要点及案例分析：

侵权人主观恶意显著、重复侵权、持续时间长、侵权获利巨大，诉讼中拒不配合勘验、拒不提交证据构成举证妨碍，属于情节严重，符合惩罚性赔偿适用条件。法院以惩罚性赔偿法律施行前的利润总额为基数，按 30% 技术贡献率确定补偿性赔偿；以施行后利润总额为基数，适用 2 倍惩罚性赔偿。同时针对持续侵权、违背承诺、拒不履行停止侵害义务等情形，设定高额迟延履行金，强化裁判执行与惩戒效果。

（五）刑事及行政维权相关案例

案例 14 刑事严惩侵害商业秘密犯罪，护航新质生产力

案号：（2024）沪 03 刑初 67 号

审理法院：上海市第三中级人民法院

要点及案例分析：

权利公司的涉案芯片设计技术信息不为公众所知悉、具有商业价值且权利人采取保密措施，符合商业秘密三性要件。被

告的创始团队利用曾在权利公司处担任高管和核心研发人员的便利，在离职后设立某科技公司，以支付高薪、股权利诱等方式，诱导多名原权利公司研发人员跳槽至其公司，并指使这些人员在离职前通过摘抄、截屏等方式非法获取权利公司芯片技术信息，抄袭并运用于被告公司设计的同类型芯片上，企图以此非法牟利。上海警方联合专业部门的鉴定结果显示，侵权芯片技术有 40 个技术点与权利公司商业秘密的密点具有 90% 以上同一性，构成实质性相同。法院根据 10 余名被告人在非法获取、使用技术秘密中的地位、作用、参与程度，区分主从犯并依法量刑。刑事维权途径惩处力度强、可采取技术侦查等强制措施、预防效果突出，能够有效打击严重侵害商业秘密犯罪行为。

案例 15 行政重拳出击，打击非法泄密

案号：沪市监黄处（2025）012024000482、483 号

处理机关：上海市黄浦区市场监督管理局

要点及案例分析：

当事人丛某某在权利人公司任职期间，违反保密义务，利用职务便利将公司两份内部管理流程文件存储在个人电脑内，并带至新公司保存在电脑内。同时，在丛某某已经离职的情况下，当事人张某某应丛某某之要求，违反公司保密义务，利用微信向其传输四份企业内部管理流程文件。两名当事人明知上述六份文件属于当事人的经营秘密，却违反保密义务，利用职务便利传输、保存相关涉密文件，致使原公司的经营秘密承受失控的风险，该行为违反了在职期间签署的保密协议及员工手册相关规定。经鉴定，涉案六份文件与原始内部文件实质相同且不为公众所知悉并具有商业价值，故应认定两当事人实施了侵犯商业秘密的行为。行政机关责令两名当事人立即停止违法

行为，并分别罚款人民币 200000 元，合计 400000 元。行政维权途径具有高效快捷、依职权主动调查、成本相对较低等优势，可及时阻断侵权信息扩散。