上海市松江区人民法院

欢迎关注松法官方
微信公众号



松法·护航区域社会发展系列规范指引

商业秘密保护规范指引

上海市松江区人民法院

2026年9月

前言

商业秘密是企业知识产权体系中的核心构成，是维系市场竞争优势、驱动创新发展与实现可持续经营的关键战略资产。在商业秘密的全流程保护过程中，既要依法筑牢企业商业秘密保护屏障，保障权利人合法权益与核心竞争力，亦需兼顾保障劳动者正当劳动权益、择业自由与职业发展权利，实现商业秘密保护与劳动者合法权益的有机统一。加强商业秘密保护，不仅关乎权利人的合法权益，更关系到市场公平竞争秩序、创新发展生态、营商环境建设。当前全球产业竞争日趋激烈，商业秘密侵权形式日益复杂，加强商业秘密保护，打造良好的创新创业生态，统筹推进商业秘密严格保护与劳动者权益保障，对于我国企业融入国际贸易秩序、取得国际竞争优势具有重大意义。上海市松江区作为长三角G60科创走廊策源地，围绕新质生产力发展先行区的功能定位，长期致力于打造保护创新的法治化营商环境。为进一步提升科创企业的商业秘密规范化保护水平，引导企业在合法合规框架内完善保密机制、防范法律风险，同时规范权利边界、保障劳动者正当权益，提升企业在国际化市场竞争中的竞争优势，推动产业升级和高质量出海，上海市松江区人民法院梳理司法办案实践，结合侵犯商业秘密司法案件中的常见问题，发布商业秘密保护与风险防范指引，着力为技术创新突破、产业迭代升级、劳资权益平衡营造更加公平、规范、可预期的法治化营商环境。

目录

一、商业秘密的基本概念及司法认定.....1

二、构建“实质有效”的保密措施体系.....10

三、侵犯商业秘密行为的认定.....23

四、侵犯商业秘密的司法救济方式.....36

五、提升企业商业秘密保护意识.....47

一、商业秘密的基本概念及司法认定

问1：什么是商业秘密？

答：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。由此可见，商业秘密包括技术秘密和经营秘密两种。

商业秘密的法定构成要件包括：（1）秘密性：信息不为所属领域的相关人员普遍知悉，且不能从公开渠道容易获得，若信息属于行业常识、已公开披露或通过公开渠道容易获得，则不具备秘密性。**（2）**价值性：信息因其秘密性而具有现实或潜在的商业价值，能为权利人带来经济利益或竞争优势。**（3）**保密性：权利人采取了与信息商业价值、获取难度相适应的合理保密措施，以防止信息泄露，如签订保密协议、限制信息接触范围、对载体加密等。未采取合理保密措施的信息不受法律保护。

问2：如何认定商业秘密“不为公众所知悉”？

案例索引：某信息科技公司于2012年推出“某某精灵”，在红外遥控方面积累了一定经验。2013年，某终端公司与某信息科技公司为手机实现红外控制目的签订《相互保密协议》，并由某终端公司与某信息科技公司就手机红外控制功能实现进行了联调。原告某信息科技公司起诉称某终端公司以订立商业合同、给予交易机会为由，获取原告的红外遥控技术秘密，侵害了其红外遥控技术秘密。被告抗辩称原告请求保护的技术秘密已为公众所知悉，不具有非公知性。法院生效裁判认为，原告主张的相应技术秘密，部分已被他人申请相关专利并进行公开，部分技术秘密在期刊文章或网络中有载明，属于现有技术领域内的公知常识。原告的主张除个别秘点外，其余均为公众所知悉。因此，驳回原告大部分秘点构成商业秘密的诉讼主张。[1]

答：构成商业秘密的技术信息或经营信息应当

1. 参见上海市高级人民法院（2021）沪知民初4号、最高人民法院（2024）最高法知民终904号民事判决书。

具有秘密性。在对“不为公众所知悉”的把握上，需要注意的是，下列情形会被认定相关信息属于“为公众所知悉”，不构成商业秘密：

(1) 该信息在所属领域属于一般常识或者行业惯例的；

(2) 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；

(3) 该信息已经在公开出版物或者其他媒体上公开披露的；

(4) 该信息已通过公开的报告会、展览等方式公开的；

(5) 所属领域的相关人员从其他公开渠道可以获得该信息的。

需要注意的是，对上述为公众所知悉的信息进行整理、改进、加工后形成的新信息，如果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，仍可以构成商业秘密。

问3：如何认定商业秘密具有“价值性”？

案例索引：被告系原告公司员工，原告起诉称被告在其公司工作期间窃取公司对外签订的大量合同信息，披露合同中的销售价款、销售毛利率等保密信息，并将公司内部机密邮件、内部绩效考核制度披露给第三方，侵害原告的商业秘密。被告辩称销售合同信息、考勤邮件等均不属于商业秘密，即使披露了也不会对市场竞争秩序和原告的企业竞争优势造成威胁。法院生效裁判认为，考勤信息等对公司内部具有普遍的秘密性，该信息对公司运营可能具有一定价值，但原告未能证明上述信息可以为其带来直接、积极的竞争优势，故不具有经营秘密意义上的价值性。[2]

2. 参见上海知识产权法院（2022）沪73知民初945号、上海市高级人民法院（2024）沪民终567号民事判决书。

答：《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》（以下简称《商业秘密司法解释》）第七条规定，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。第十九条第二款规定，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。符合下列情形之一的，可以认定为该信息能为权利人带来商业利益或竞争优势，具有相应的价值性：

（1）该信息可以给权利人带来经济收益或者产生竞争优势；

（2）该信息对其生产经营具有重大影响；

（3）权利人为获得该信息，支付相应对价、产生研发成本或者经营成本以及有其他物质投入的；

（4）其他能证明该信息能为权利人带来商业利益或竞争优势的。

需要注意的是，价值性的认定，应以信息能否带来竞争优势作为判断标准，不论是已经实际应用的信息，还是尚未直接应用但可以避免企业“走弯路”的信息，只要能够带来竞争优势，一般均符合价值性的要求。

问4：如何认定权利人采取了“相应保密措施”？

案例索引：原告某信息科技公司针对其主张的商业秘密，制定相关保密制度文件，规定保密范围、密级确定、保密措施等。同时与员工签署《劳动合同》《保密合同》，明确员工在任职期间及离职后应保守公司技术秘密和其他商业秘密，对研发部员工离职后的竞业限制义务进行了约定。原告同时与被告某技术有限公司等签订《相互保密协议》约定相关保密信息。被告认为，《相互保密协议》约定的保

密信息的范围仅限于记载有保密标识的书面形式披露的信息，原告对涉案商业秘密未以书面形式披露或确认任何添加有保密标识的保密信息，亦未以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围，未对涉密载体进行区分和管理。法院生效裁判认为，原告虽与被告签订《相互保密协议》，且公司内部制定《保密制度》《企业员工保密合同》等文件，但未有证据显示原告将其主张的相关技术秘密交付给被告，亦未在任何信息中标明保密字样，且存在邮件发送秘点文件未标注“保密”情况，原告主张作为技术秘密载体的部分电子文件均非原始电子文档，且存储于其家庭用电脑文件夹内，未对载体进行区分和管理。因此现有证据不足以证明原告就涉案技术秘密采取了与其主张技术秘密商业价值相适应的合理保密措施，判决驳回原告全部诉讼请求。[3]

答： 企业作为商业秘密权利人，除内部制定保密制度、外部签订保密协议外，应重点围绕“秘点”采取

3. 同前引1。

相应的保密措施：

（1） 对“秘点”技术或者信息设定密级、保密期限和知悉范围，进行分级管理；

（2） 对涉密载体采取加密、加锁等预防措施或者其他加密管理措施，如可以贴附保密标识或者秘密提示；

（3） 对涉密场所及涉密设备采取访问限制等物理隔离措施进行管理；

（4） 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；

（5） 与离职员工签订竞业限制协议，并给予合理足额的经济补偿，要求员工离职后继续保守商业秘密；

（6） 采取其他合理保密措施。

【温馨提示】 权利人主张构成商业秘密的技术

信息或经营信息（秘点），并不具有通用的形式，亦不需要具有实用性。权利人提供证据证明技术信息或经营信息符合商业秘密的三要件，即可认定构成商业秘密。对技术研发信息而言，失败的实验数据与成功的技术方案同样具有商业秘密的价值性，可以纳入到商业秘密中进行保护。对经营信息而言，权利人若主张相关客户信息以及客户交易习惯构成商业秘密的，应对该经营信息进行提炼、总结，通过相应的保密载体予以体现，并采取相应的保密措施。

二、构建“实质有效”的保密措施体系

问5：如何构建商业秘密保护管理制度？

案例索引：原告主张其生产工艺构成技术秘密，并称已通过员工手册提出保密要求，但未能举证证明将《员工手册》送达员工并进行公示，也未提交证据证明其对涉案工艺信息采取了分类标记、权限限制等针对性管理措施。被告抗辩称原告未就涉案信息采取有效保密措施。法院生效裁判认为，权利人主张采取了保密措施的，应当举证证明相关制度已实际执行且能够被涉密人员感知。原告仅提交笼统的保密原则性规定，未针对涉案商业秘密建立具体管理规范，无法证明已向涉密人员有效告知相关制度规定，不足以体现其保密意愿与防控效果，故认定其未采取相应保密措施，涉案信息不构成商业秘密。[4]

4. 参见最高人民法院（2022）最高法知民终2581号民事判决书。

案例索引：上海某知识产权服务公司主张其客户名单、交易报价等经营信息构成商业秘密。该公司在《劳动合同》中明确约定了商业秘密的具体范围，《员工手册》规定员工不得私自拷贝、存储公司涉密信息，同时对员工办公电脑安装监控系统管控信息传输。公司销售人员吴某在职期间，将涉密客户信息与交易机会泄露给其关联方，促成“飞单”交易并收受回扣。法院生效裁判认为，权利人通过劳动合同明确保密范围、员工手册细化行为禁令、技术手段管控信息传输，形成了制度与技术结合的完整保密管理体系，相关措施可被员工明确感知且具备可执行性，应当认定已采取相应保密措施，涉案经营信息符合商业秘密法定构成要件。[5]

答：根据《商业秘密司法解释》的规定，人民法院认定保密措施效力时，将综合考量商业秘密载体性质、商业价值、保密措施可识别程度、与商业秘密的对应程度及权利人保密意愿等因素。合法有效的保密管理制度应当具备明确性、针对性与可执行性。仅笼统约

5. 参见上海市松江区人民法院（2025）沪0117民初12997号民事判决书。

定“员工应当保守公司秘密”而无具体规则与执行机制的，难以被认定为采取了相应保密措施。因此，企业在制定商业秘密保护管理制度时，应注意以下几点：

（1）明确范围与分级分类。制定企业自身商业秘密管理办法，清晰界定技术信息、经营信息的具体范围，按照秘密重要程度划分为核心秘密、重要秘密、一般秘密三级，并对应不同的知悉权限、防护标准与管理流程；

（2）建立全流程管控规范。覆盖商业秘密的产生、存储、传输、使用、销毁全生命周期，明确涉密文件的标记、归档、借阅、复制、销毁规则，以及涉密信息的内部传输渠道与审批流程；

（3）明确责任与追责机制。指定保密管理责任部门与涉密岗位责任人，将保密义务纳入岗位职责与绩效考核。明确违反保密制度的内部惩戒措施，以及造成泄密后的追责路径；

（4）留存制度执行痕迹。定期开展保密制度宣贯与考核，保留培训记录、审批单据、检查台账等书面证据，确保制度并非“纸面化”存在。

问6：如何加强对涉密人员的管理？

案例索引： A集团下属的成都高某公司近40名高级管理人员及技术人员于2016年先后离职，至B集团及其关联公司工作。A集团发现B集团及其关联公司以上述部分离职人员作为发明人或者共同发明人，利用其在成都高某公司工作期间接触、掌握的有关新能源汽车底盘应用技术，以及其中的12套底盘零部件图纸、数模承载的技术信息申请了12件实用新型专利。B集团及其关联公司在没有任何技术积累或者合法技术来源的情况下，短期内推出包括威某EX5等型号在内电动汽车，涉嫌侵害A集团案涉汽车底盘技术秘密。法院生效裁判认为，涉案员工在成都高某公司产品管理或者技术岗位从事相关工作，均与成都高某公司签订了《劳动合同》及《保密协议》，《劳动合同》文本为A集团统一的格式合同。A集团建设了协同办公系统（CPC），供员工使用，该办公系统设置了密码权限管理制度。成都高某公司相当数量离职员工进入B集团及其关联公司工作，有些还担任了B集团及其关联公司的高级管理人员。上述离职员工均负有保密义务，并且能够接触到涉案底盘零部件技术图纸。B集团及其关联公司应当知道其所招募的离职员工应对原单位所接触的零部件图纸具有保密义务，仍然在制造涉案电动汽车时使用原告享有商业秘密的技术图纸，构成对原告商业秘密的侵害，依法应当承担停止侵害的责任。[6]

案例索引： 被告李某原系原告公司技术人员，在职期间通过公司邮件系统，将其接触到的车辆制动控制技术秘密及经营信息发送至个人邮箱。法院生效裁判认为，原告通过劳动合同保密条款、IT安全手册等方式对涉案信息提出保密要求，且明确了员工的信息传输与使用规范，已采取合理保密措施。被告在任职期间，未经许可将涉密信息从公司系统转至个人存储渠道，使商业秘密脱离原告控制，产生被披露、使用的风险，属于以不正当手段获取商业秘密的侵权行为。[7]

6. 参见最高人民法院（2023）最高法知民终1590号民事判决书，本案为最高人民法院案例库入库案例，入库编号：2026-18-2-189-001。

7. 参见上海知识产权法院（2022）沪73知民初945号民事判决，本案系2026年上海法院涉商业秘密保护十大典型案例。

答：涉密人员是商业秘密泄露的高风险主体。司法实践中，企业对涉密人员的管理措施是否到位，是判断保密措施是否合理的重要考量因素之一。针对不同层级涉密人员采取差异化的权限管控与义务约束，且相关管理措施能够被员工明确知晓的，通常会被认定为有效保密措施。企业在涉密人员管理过程中，应注意以下几点：

（1）入职环节前置管控。对核心涉密岗位开展背景调查，确认候选人不负有对前单位的竞业限制与保密义务。入职时同步签订《保密协议》，明确保密范围、义务内容与违约责任，对核心岗位可同时签订《竞业限制协议》；

（2）在职期间权限分级。按照“最小必要”原则设定信息访问权限，核心商业秘密仅向必需岗位开放。定期对涉密人员开展保密培训与警示教育，留存培训签到与考核记录；

（3）离职环节闭环管理。员工提出离职后立即调整其信息访问权限，开展离职保密谈话，要求其签署《离职保密承诺书》，清点并返还全部涉密载体，明确离职后的保密义务与竞业限制义务并按约

支付合理的竞业限制补偿，留存全部交接记录。

问7：如何加强对涉密区域的管理？

案例索引：原告某石英玻璃公司主张案涉技术信息构成技术秘密，陈某某非法披露、使用并允许某光电科技公司使用其技术秘密，某光电科技公司与肖某某明知陈某某系原告前员工并掌握原告的技术秘密，却仍非法获取、使用该技术秘密。被告辩称，原告未对案涉技术信息的载体采取符合其自身规定的保密措施。法院生效裁判认为，原告印发《档案室保密条例》，严格限制、规范档案借阅流程，将存放技术资料的档案室列为涉密区域，限制无关人员进入，同时印发《保密条例》，明确规定公司的保密范围、限制人员随意进入涉密区域、竞业限制和相应奖惩措施。被告陈某某自认收到公司的保密文件，相关证人证言亦证明原告的员工知晓自身具有保密义务。原告关于保密措施的证据充分，能

够使员工感知公司对技术信息予以保密的意愿，并且相应措施具有可识别性和操作性，且证据记载保密措施采取的时间在陈某某任职期间，符合被诉侵权行为发生以前的要件。[8]

答：根据《商业秘密司法解释》的规定，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，属于法定的有效保密措施情形。司法实践中，区域隔离的物理边界是否清晰、出入管控是否严格、访客管理是否规范，是法院审查的重点，也是权利人应重点采取的措施。企业在涉密区域管理中，应注意以下几个方面：

（1）物理隔离分区管理。将生产车间、研发实验室、数据机房等涉密区域与公共办公区物理隔离，设置门禁、围栏等物理屏障，区分不同密级区域的准入权限；

（2）严格出入管控机制。涉密区域实行人员权限准入制度，仅限授权人员进入。访客进入需履

8. 参见最高人民法院（2023）最高法知民终2467号民事判决书。

行审批、登记手续，由专人全程陪同，限制携带摄影、存储设备，明确禁止接触的区域与信息；

（3）监控与留痕管理。在涉密区域出入口及关键点位安装视频监控，留存出入记录与监控录像。对涉密区域内的文件、设备移动进行审批登记，确保涉密信息可追溯。

问8：如何加强对涉密设备的管理？

案例索引：被告人张某原系鼎某公司副总裁、首席科学家，双方签订《保密及工作成果协议》。张某任职期间违反公司规定，擅自备份公司FM芯片设计的全部数据库文件，离职后设立芯某公司，使用上述技术秘密生产同类芯片并对外销售，造成权利人重大经济损失。法院生效裁判认为，鼎某公司对涉案芯片技术数据采取了数据库权限管控、保密协议约定等管理措施，涉案信息构成商业秘密。张某违反公司设备管理规定，擅自备份涉密数据库并用于同业经营，其本

人及设立的芯某公司均构成侵犯商业秘密罪，依法承担刑事责任。[9]

答：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、存储设备等采取禁止或者限制使用、访问、存储、复制等措施的，属于法定的有效保密措施。司法实践中，设备管控的核心是实现“涉密信息不落地、外传可追溯”，仅作口头要求而无技术或制度限制的，难以认定为有效措施。对涉密设备，企业作为权利人可以采取以下措施进行管理：

（1）设备分级与权限管控。对涉密计算机、存储设备统一登记编号，按照密级分级管理。关键涉密设备禁止接入公共网络，禁用USB接口、蓝牙等外接传输渠道，设置开机密码与文件加密；

（2）传输与复制审批制。涉密信息的内部传输限定于公司指定系统，禁止通过个人邮箱、即时通讯工具传输涉密文件。涉密文件的复制、导出需履

9. 参见上海市浦东新区人民法院（2009）浦刑初字第1766号刑事判决书。

行审批流程，留存操作日志与审批记录；

（3）设备全生命周期管理。涉密设备的维修、报废需履行审批程序，报废时对存储介质进行物理销毁。员工离职时，全面清退其办公设备中的涉密信息，注销系统账号与访问权限。

问9：如何加强企业在业务合作中的商业秘密管理?

案例索引：某实业公司与模具厂签订《模具采购合同》，约定模具厂对实业公司提供的设计图纸负有保密义务，合同履行完毕后应归还资料且不得留存。后模具厂员工徐某违反保密约定，将涉案技术图纸披露给某体育用品公司，该公司据此申请专利并公开，导致商业秘密泄露。法院生效裁判认为，合同约定的保密条款合法有效，合作方及其工作人员均负有明确的保密义务。违反合同约定将商业秘密披露导致商业秘密被公开的，构成侵害商业秘密。第

三方明知信息来源违法仍获取并使用的，构成共同侵权，依法承担连带赔偿责任。同时，合同保密条款可作为权利人已采取保密措施的直接证据，具有免证效力。[10]

答： 根据法律规定，业务合作方基于合同关系知悉权利人商业秘密的，负有约定及法定的保密义务。司法实践中，权利人是否在合作前明确保密要求、是否限定信息披露范围、是否约定合作后的返还与销毁义务，是判断保密措施是否到位的核心标准，也是对合作方泄密后追责的关键依据。对外合作中，企业可采取以下措施强化商业秘密管理：

（1） 保密协议前置签署。在技术合作、委托加工、供应链协作等业务开展前，先行签署《保密协议》或在合作合同中设置专门保密条款，明确保密信息范围、使用限制、保密期限及违约责任；

（2） 信息披露分级管控。按照“最小必要”原则向合作方披露信息，仅提供合作必需的内容，避免重要秘点全盘披露。对交付的涉密文件标注保密标识，限定接触人员与使用场景；

10. 参见最高人民法院（2022）最高法知民终1981号民事判决书。

（3） 合作后闭环管理。合作终止时，要求合作方返还全部涉密载体，删除存储的涉密信息并出具确认函。明确约定合作终止后的保密义务仍持续有效，不得擅自披露、使用或允许第三方使用相关信息。

【温馨提示】 保密措施是商业秘密的“防护盾”，也是司法保护的“准入门槛”。实践中，不少企业存在“重协议、轻执行”“重形式、轻实质”的误区，仅靠一份笼统的保密协议便认为完成了保密管理，最终因举证不能无法获得司法救济。

企业构建保密措施体系，应当遵循“实质有效”原则，围绕“人、物、场、流程”等多个维度形成闭环。即人员管理要覆盖入职到离职全周期，载体管理要落实技术管控与制度约束，区域管理要实现物理隔离与权限分级，对外合作要做到保密前置与全程留痕。唯有将保密要求嵌入日常经营的每个环节，才能在纠纷发生时有效举证，真正守住企业的无形资产。

三、侵犯商业秘密行为的认定

准确认定侵犯商业秘密行为，是企业开展维权、司法机关适用法律的关键前提。《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》）第十条系统规定了四类侵犯商业秘密的法定行为，同时明确第三人在明知或应知情形下视为侵犯商业秘密的认定，涵盖了从非法获取、披露使用到教唆帮助的全链条侵权行为。

问10：哪些行为构成侵害商业秘密？

案例索引：华某、刘某等原系天某公司员工，任职期间掌握公司某产品生产工艺技术秘密。二人离职后加入纽某公司，将所掌握的技术秘密披露给该公司，纽某公司利用该技术秘密生产同类产品并对外销售。法院生效裁判认为，华某、刘某违反保密义务，向第三方披露并允许其使用权利人商业秘密，构成违反保密义务类侵权行为，纽某公司明知二人系以不正当手段披露技术秘密，仍获取并大规模使用，属于第三人恶意获取使用商业秘密的情形，同样构成侵权。各主体依据其在侵权链条中的作用，承担相应的连带赔偿责任。[11]

案例索引：吴某系松江区某知识产权服务公司销售人员，掌握公司客户名单、报价体系、项目进度等经营信息。其在职期间，将正在跟进的客户项目信息泄露给其好友孔某实际控制的多家同业公司，截留客户交易机会并促成“飞单”，从中收受回扣。法院生效裁判认为，吴某违反保密义务，擅自披露、允许他人使用其所掌握的商业秘密并牟取私利，属于 2019年《反不正当竞争法》第九条规定的违反保密义务类侵权行为。孔某及其控制的公司明知信息来源违法仍获取并使用，构成第三人侵权，二者均应当承担侵权责任。[12]

11. 参见最高人民法院（2019）最高法知民终562号民事判决书，本案系最高人民法院第219号指导性案例。

12. 参见上海市松江区人民法院（2025）沪0117民初12997号民事判决书。

答：根据《反不正当竞争法》第九条的规定，侵害商业秘密的行为包括四类法定情形，经营者以外的自然人、法人、非法人组织实施下列行为的，均视为侵犯商业秘密：

（1）非法获取行为，即以盗窃、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；

（2）非法披露、使用行为，即披露、使用或者允许他人使用以前项不正当手段获取的权利人的商业秘密；

（3）违反保密义务的行为，即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；

（4）教唆帮助行为，即教唆、引诱、帮助他人违反保密义务或者权利人的保密要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

此外，第三人明知或者应知商业秘密系他人非法获取，仍获取、披露、使用或者允许他人使用的，也视为侵犯商业秘密。

企业发现商业秘密被侵害时，可先对照上述法定情形固定侵权行为证据，针对不同侵权主体的行为分别取证，既可主张直接侵权人承担责任，也可追究第三人的连带责任。

问11：如何认定获取商业秘密的“不正当手段”？

案例索引：孙某任职于沈某集团期间，通过配偶隐名持股设立同业公司斯某公司，利用职务便利获取公司离心压缩机选型软件及核心技术数据，交由斯某公司用于同类产品经营。法院生效裁判认为，员工在职期间隐瞒身份设立同业竞争企业，利用岗位权限秘密获取原单位商业秘密并用于经营，本质上违背了忠实义务与公认商业道德，属于以“其他不正当手段”获取商业秘密的情形，依法构成侵权。[13]

13. 参见最高人民法院（2022）最高法知民终1592号民事判决书，本案系2025年最高人民法院反不正当竞争典型案例。

答：“不正当手段”的认定以违反法律规定、违背公认商业道德为核心判断标准。除盗窃、贿赂、欺诈、胁迫、电子侵入等明确列举的情形外，凡以违反诚实信用原则和公认商业道德的方式获取他人商业秘密的，均属于不正当手段，包括但不限于：通过利诱企业员工获取、利用合作关系套取、以反向工程为名非法拆解涉密设备、通过黑客技术侵入信息系统等。

司法实践中适用“接触+实质相同-合法来源”认定规则。若权利人能证明被诉侵权人接触过商业秘密，且其使用的信息与商业秘密实质相同，同时被诉侵权人无法说明信息合法来源的，可推定其系以不正当手段获取。

企业招聘竞争对手离职员工、开展同业合作时，应当严格审查信息来源合法性，避免因“明知或应知”信息来源非法而落入侵权范畴。

问12：如何认定披露、使用商业秘密行为?

案例索引：某集团公司通过利诱权利人某化工公司员工，非法获取香兰素生产的全套设备图与工艺流程图，随后建设生产线生产同类产品并销售。诉讼中某集团公司抗辩称仅参考了部分技术，未使用全部商业秘密。法院生效裁判认为，权利人已举证证明被诉侵权人非法获取了完整的生产技术秘密，且实际生产出了相同产品，被诉侵权人未能举证证明其系通过自主研发获得技术，故应当认定其使用了全部涉案技术秘密。对技术秘密的修改、调整不影响使用行为的认定。[14]

答：披露行为指将商业秘密告知第三方或擅自将商业秘密公开，既包括向特定对象泄露，也包括向不特定公众公开。既包括主动告知，也包括在未采取保密措施的场合放任信息扩散。披露行为一旦实施，无论是否造成实际获利，均构成侵权。使用行为指将商业秘密用于生产经营活动，既包括直接原样使用，也包括修改、调整后使用。既包括用于

14. 参见最高人民法院（2020）最高法知民终1667号民事判决书，本案系最高人民法院第220号指导性案例。

生产产品，也包括用于优化经营策略、争取交易机会等。

若权利人举证证明被诉侵权人非法获取了完整的工艺流程、成套技术资料等商业秘密，且已生产出相同产品，可推定其使用了全部商业秘密，被诉侵权人不能作出合理解释的，应当承担侵权责任。

问13：保密义务具体有哪些要求？

案例索引：魏某、胡某系原告公司高级管理人员，掌握公司核心客户名单等经营秘密，但双方未单独签订保密协议。二人离职后，向第三方披露并允许其使用上述客户信息开展同业经营。诉讼中二人辩称未签订保密协议，不负有保密义务。法院生效裁判认为，公司高级管理人员基于职务身份与忠实义务，理应知晓核心经营资源属于公司秘密信息，即使未单独签订保密协议，也依据诚实信用原则与公司法上的忠

实义务负有法定保密义务。违反该义务披露、允许他人使用商业秘密的，同样构成侵权。[15]

案例索引：尹某系松江区某外贸公司业务员，双方劳动合同与保密协议均约定，员工在职及离职后均需对公司客户信息、采购渠道等经营信息承担保密义务。尹某在职期间隐名设立同类贸易公司，利用职务便利将公司客户与供应商资源导流至自有公司，截留订单获利。法院生效裁判认为，双方已通过书面合同明确约定保密义务范围与期限，尹某在职期间利用岗位便利私自使用公司经营资源牟利，违反了约定的保密义务与劳动者忠实义务，应当承担违约与侵权责任。即使未单独签订保密协议，基于劳动关系的人身信赖属性，员工对任职期间接触的核心经营信息也负有默示保密义务。[16]

答：根据《商业秘密司法解释》第十条的规定，保密义务包括两类。一是约定保密义务。通过劳动合同、保密协议、商务合同等书面方式明确约定的保

15. 参见最高人民法院（2021）最高法知民终312号民事判决书。

16. 参见上海市松江区人民法院（2024）沪0117民初22263号民事判决书。

密义务，义务范围、期限、责任以约定为准。二是法定/默示保密义务。即使无书面约定，根据诚信原则、合同性质、交易习惯等，被诉侵权人知道或者应当知道信息属于商业秘密的，也负有保密义务，例如企业高管的法定忠实保密义务、合同履行中的附随保密义务、离职员工的后合同保密义务等。

负有保密义务的人员不得擅自披露商业秘密、不得擅自使用或允许他人使用商业秘密、应当采取合理措施防止信息泄露。保密义务不因劳动合同终止、合作结束而自动消灭，只要商业秘密未公开，义务人就应当持续遵守保密义务。

问14：如何认定共同侵害商业秘密？

案例索引：尹某原系四川某化工公司员工，违反保密约定将涉案蜜胺生产技术秘密披露给宁波某咨询公司，该咨询公司将技术转售给山东某化工公

司用于生产线建设，宁波某化工设计公司明知技术来源非法，仍协助完成工程设计。四方主体分别处于侵权链条的不同环节，共同造成技术秘密泄露与使用。法院生效裁判认为，各被诉侵权人虽未全部事前共谋，但彼此知晓技术信息的违法来源，各自实施的行为前后衔接、环环相扣，共同促成了商业秘密的非法流转与使用，具有共同过错，构成共同侵权，依法对权利人的损失承担连带责任。[17]

答：共同侵害商业秘密的核心认定标准是各侵权主体之间存在共同过错，且各自行为相互配合形成完整侵权链条，共同造成损害后果。以下情形属于共同侵害商业秘密行为：

（1）共同故意侵权。各方主体事前共谋、分工协作，共同实施获取、披露、使用商业秘密的行为，最典型的如离职员工与新用人单位通谋，共同利用原单位商业秘密经营；

（2）共同过失侵权。各主体均未尽到合理注

17. 参见最高人民法院（2022）最高法知民终1129号民事判决书。

意义务，共同导致商业秘密泄露，例如合作双方均未落实保密措施导致信息扩散；

（3）故意与过失结合。部分主体主动实施侵权，部分主体未尽保密义务为侵权提供便利，二者行为结合造成损害后果的，也可构成共同侵权。

构成共同侵权的，各侵权人应当对权利人的损失承担连带责任，法院可根据各主体的过错程度、行为对损害结果的原因力大小划分内部责任份额。

问15：如何认定教唆、引诱、帮助侵犯商业秘密行为?

案例索引：孙某、印某在职期间隐名设立斯某公司，非法获取沈某集团的技术秘密用于经营。吴某明知上述技术信息来源违法，仍参与斯某公司的技术研发工作，为侵权产品的生产提供技术支持与

帮助。法院生效裁判认为，吴某明知斯某公司使用的技术系以不正当手段获取的商业秘密，仍参与其中并提供技术帮助，属于帮助他人实施侵犯商业秘密的行为，与直接侵权主体构成共同侵权，依法承担相应的侵权责任。[18]

答：教唆、引诱行为指故意以劝说、利诱、职位许诺、高额报酬等方式，唆使、诱导负有保密义务的人员违反保密要求，向其披露、提供商业秘密的行为。核心要件是行为人主观上具有教唆故意，客观上实施了诱导行为，且被教唆人因此实施了侵权行为。帮助行为是指为他人实施侵犯商业秘密行为提供便利条件、技术支持、物质帮助等，例如提供存储设备、传输渠道、技术解读服务，或为侵权产品生产销售提供场地、资质等。

教唆、引诱、帮助行为均属于共同侵权的特殊形态，行为人应当与直接侵权人承担连带责任。

18. 参见最高人民法院（2022）最高法知民终1592号民事判决书，本案系2025年最高人民法院反不正当竞争典型案例。

【温馨提示】侵犯商业秘密的行为链条长、主体多、手段隐蔽，是此类案件维权的难点所在。司法实践中，侵权行为早已从单一的“员工跳槽带密”，发展为“内外勾结、分工协作”的链条化模式，覆盖了利诱获取、中转披露、生产使用、销售获利等多个环节。

企业在经营中一方面要守住自身底线，不得通过挖角、利诱等不正当手段获取竞争对手的商业秘密，不得恶意使用来源不明的技术信息与经营信息；另一方面，在发现侵权时应全面梳理侵权链条，将处于不同环节的教唆者、提供者、使用者、帮助者一并列为追责对象，最大限度挽回自身损失，遏制全链条侵权行为。

四、侵犯商业秘密的司法救济方式

问16：商业秘密受到侵害时如何进行取证？

案例索引：原告松江区某知识产权服务公司在分配给员工的工作电脑（涉密载体）中安装了办公电脑监控系统，对员工日常工作进行相应监控。原告在发现商业秘密被侵害后，通过电子取证向法院提交涉密载体中被告吴某将相关订单的秘密信息发送给其好友的记录，从而固定侵权行为，后法院经审理认定被告侵害商业秘密行为成立，依法判决被告停止侵权并赔偿经济损失。[19]

答：企业在对商业秘密采取保护措施的同时，应当注意预防并搜集可能存在侵害商业秘密行为的证据，避免在进行维权时因缺乏证据而导致败诉。具体应注意以下几点：

19. 参见上海市松江区人民法院（2025）沪0117民初12997号民事判决书。

（1）发现涉嫌侵害商业秘密行为时，通过可信时间戳、数字存证等方式第一时间搜集涉及侵害商业秘密行为的聊天记录、电子邮件、网页截图等相关证据，防止证据灭失；

（2）对可能销毁或者不易保存的证据，可邀请公证机关至现场，对侵权人实施发行、销售侵权物品等相关行为进行公证取证；

（3）可向有管辖权的市场监督管理部门进行举报并提供初步证据、侵权线索，申请行政查处，后续可调阅行政机关在查处过程中形成的场所检查记录、询问当事人、证人笔录、扣押清单等证据；

（4）若侵害商业秘密的行为涉嫌犯罪，可向公安机关报案。

问17：侵犯商业秘密可能承担何种民事责任？

案例索引：原告上海某科技有限公司系一家开

发、运营网络游戏的公司，在每次游戏版本更新前均会招募玩家进行测试，并对测试内容与玩家签订保密协议，对测试内容采取了必要、合理的保密措施。吴某系知名游戏资讯博主，其从一个分享泄密物料的QQ群中获得该游戏尚未公开版本的安装包，按照教程安装后运行游戏进行试玩，并将试玩过程录制成视频发布到抖音平台。法院生效裁判认为，涉案游戏新增的场景画面、剧情设定等信息系游戏运营过程中的核心资源，能够给权利人带来竞争优势，具有较高的商业价值，在被诉侵权行为发生之时不为公众所知悉，且已被采取了必要、合理的保密措施，构成反不正当竞争法所保护的商业秘密。吴某明知或者应知其所获取的系他人以不正当手段获取的商业秘密，但仍获取、披露该商业秘密，该行为应视为侵犯原告享有的商业秘密，应承担消除影响、赔偿损失的法律责任。[20]

答：侵犯商业秘密的民事责任主要包括停止侵权、消除影响和赔偿损失。企业在商业秘密受到侵

20. 参见上海市徐汇区人民法院（2024）沪0104民初12537号民事判决书，本案2026年上海法院涉商业秘密保护十大典型案例。

害时，可以根据具体情形向侵权方主张相应的民事责任，具体指引如下：

（1）被诉侵害商业秘密的行为在起诉时尚未停止的，可以要求侵权人立即停止披露、使用或允许他人使用其接触或获取的商业秘密，防止损害后果进一步扩大；

（2）要求侵权人返还或销毁侵权载体，包括含有商业秘密的资料、物品等载体，并清除其控制的商业秘密信息；

（3）被诉侵权行为对商业秘密权利人的商誉、信誉造成损害的，可要求侵权人在一定范围内采取发布声明等方式消除不良影响；

（4）要求侵权人赔偿因侵权行为给权利人造成的经济损失。《反不正当竞争法》第二十二条规定，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。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。

对于故意侵害商业秘密且情节严重的侵权行为，可主张适用惩罚性赔偿。主张适用惩罚性赔偿的，权利人应当明确惩罚性赔偿的计算基数及适用倍数，人民法院适用惩罚性赔偿确定的赔偿数额总额，最高为计算基数的五倍。需要注意的是，惩罚性赔偿的计算基数应当具体而明确，实践中权利人往往因无法明确计算基数而导致惩罚性赔偿的主张无法获得法律支持。关于惩罚性赔偿的计算基数，应按照以下顺序确定：

（1）原告的实际损失数额。原告可提供侵权行为发生前后的销售数据比对、财务报表或审计报告等证据证明因侵权行为导致的销售数额减少情况、利润下降情况，作为证明其实际损失的相关证据；

（2）被告违法所得数额或者因侵权所获得的

利益。原告可初步提供被告线上或线下交易数据、被告官方网站、微信公众号、产品宣传册等披露的产销量、利润等证据证明违法所得数额或者侵权获利情况，必要时可向法院申请调取被告经营的线上店铺销售数据、增值税发票等证据予以佐证；

（3）参照权利许可使用费确定。在实际损失数额、违法所得数额或者因侵权所获得的利益均难以计算情形下，人民法院可依法参照权利许可使用费合理确定惩罚性赔偿的计算基数，权利人应当提供其相关知识产权授权给他人使用的许可合同、许可费支付凭证等证据。

问18：侵犯商业秘密可能承担何种刑事责任？

案例索引：被告人张某原系海某公司射频芯片开发部门负责人，离职后成立尊某公司。公司设立前后，张某拉拢时任海某公司员工的被告人周某等人加入尊某公司。为缩短研发周期、迅速流片量

产、加快吸引融资，经被告人张某指示，被告人周某等公司管理层招募海某公司员工入职尊某公司。时任海某公司员工的被告人高某等人在明知海某公司对其技术信息采取了保密措施的情况下，仍于离职前后应尊某公司要求，自行或者勾结海某公司员工用不正当手段获取海某公司技术信息用于尊某公司芯片研发。法院生效判决认为，张某等14名被告人通过不正当手段获取海某公司的商业秘密，情节特别严重，其行为均已构成侵犯商业秘密罪，故判决各被告人有期徒刑一年至六年不等，罚金五十万元至三百万元不等的刑罚。[21]

答：侵犯商业秘密行为情节严重，权利人可以向公安机关报案，追究侵权人的刑事责任。根据《中华人民共和国刑法》第二百一十九条的规定，构成侵犯商业秘密罪的情形包括：

（1）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的；

21. 参见上海市第三中级人民法院（2024）沪03刑初67号刑事判决书，本案系2026年上海法院涉商业秘密保护十大典型案例。

（2）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；

（3）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的。

行为人明知前述情形的行为，仍获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。

问19：侵犯商业秘密纠纷举证责任如何承担？

案例索引：原告某信息科技公司认为，某终端公司通过某技术公司和某思公司，以订立商业合同、给予交易机会为由，获取原告红外遥控技术秘密，应用在某思公司的芯片和某终端公司生产、销售的手机上，侵害了其红外遥控技术秘密。被告辩

称，原告主张的技术信息缺乏载体支持，不满足商业秘密法定构成要件，且未提供证据证明三被告接触其主张的技术秘密。法院生效裁判认为，涉案技术秘密虽不为公众所知悉，但价值较低，且部分秘点载体无法反映秘点内容，载体形成时间均无法确认，无法证明被诉侵权行为发生时原告主张的涉案技术秘密已经形成，原告未举证证明被诉侵权信息与其主张的涉案技术秘密实质相同，因此判决驳回原告全部诉讼请求。[22]

答：在侵害商业秘密纠纷案件中，举证责任关涉维权能否成功、商业秘密能否获得法律保护，具有至关重要的作用。企业在商业秘密被侵害时，一般需对以下事项承担举证责任：**（1）**提供证据证明其主张的商业秘密具有秘密性、价值性，并已采取合理的保密措施；**（2）**提供初步证据证明被告具有接触商业秘密的可能性；**（3）**被告获取、披露、使用或允许他人使用的信息与原告主张的商业秘密信息构成实质性相似。

22. 参见上海市高级人民法院(2021)沪知民初4号、最高人民法院(2024)最高法知民终904号民事判决书，本案系2026年上海法院涉商业秘密保护十大典型案例。

权利人提供初步证据证明上述事项后，则相应的举证责任发生转移。即被告应提供证据证明其不存在侵犯商业秘密的行为，或者原告主张的技术信息、经营信息不构成商业秘密。具体包括：**（1）**提供证据证明权利人主张的技术信息、经营信息不符合商业秘密的构成要件（秘密性、价值性、保密性）；**（2）**提供证据证明其获取或者使用的信息来源合法，如系自主研发、通过反向工程或合法受让获得；**（3）**提供证据证明其使用的技术信息、经营信息与权利人主张的商业秘密存在实质性差异，或未披露、使用该信息。

【温馨提示】 企业的商业秘密受到侵害时，可以通过以下方式进行法律救济：

（1）行政救济：向市场监督管理部门举报，经市场监督管理部门调查后，依法进行认定查处；

（2）民事救济：申请仲裁或提起民事诉讼，要求侵权人停止侵权并赔偿损失，对恶意侵害商业秘密且情节严重的行为，可依法主张惩罚性赔偿；

（3）刑事救济：侵害商业秘密的行为情节严

重、造成权利人重大损失，涉嫌刑事犯罪的，可向公安机关报案，追究侵权人相应的刑事责任。

在维权过程中最为重要的是，及时固定并向有关机关提交证据加以证明。除前述举证责任中所列情形外，企业对于因客观原因不能自行收集的证据，可以向法院申请调查取证，对于证据可能灭失或者以后难以取得的情形，可以向法院申请进行证据保全。同时，因商业秘密受到侵害无法提供证据证明被告的侵权获利的，可以要求法院责令被告提供其销售侵权商品的相关记录，从而多维度提升维权能力。

五、提升企业商业秘密保护意识

问20：企业如何开展员工商业秘密保护教育？

答：商业秘密保护教育应贯穿员工在企全周期。对新入职员工、调岗至涉密岗位的员工应进行保密合规宣传与培训，确定其岗位涉密性质、保密义务及违规后果，培训结束后签订保密承诺书或保密协议；制定年度培训计划，面向全体员工开展定期的业务保密培训，对重点岗位、核心技术人员等开展专项保密培训；对离职、转岗、退休员工进行脱密保密培训，开展保密谈话，明确告知离职或转岗后的保密义务、禁止行为及法律责任，形成谈话记录并签字确认。

问21：企业如何确定商业秘密的秘点？

答：企业应根据行业属性、企业特点、项目特点等因素合理确定商业秘密的保护范围，避免将公知信息纳入保护范围。定秘时应综合考虑其秘密性和价值性，包括商业秘密信息的经济价值、信息对企业的重要程度、产生商业秘密信息的研发成本、对商业秘密信息采取保密措施的成本等。具体指引如下：

（1）坚持精准化与最小化原则，秘点信息应尽可能精准，恪守最小化原则，避免将公知信息纳入秘点进行保护；

（2）定期评估秘点信息的适用性与保密措施的有效性，根据经营需要或技术迭代及时更新秘点信息，确保秘点始终处于未公开状态；

（3）明确秘点信息的载体形式。商业秘密信息需通过文档、数据库等有形载体呈现，从而清晰界定商业秘密的保护范围。

问22：如何设定竞业限制协议？

案例索引：众某公司系一家从事药品检测生产、研发、销售的企业，其与不同岗位的涉密员工签订《保密合同》《竞业限制协议》，《竞业限制协议》约定员工离职后竞业限制期限、竞业范围、保密范围等。在员工离职后，众某公司向离职员工发送《竞业限制开始通知书》，明确竞业限制开始时间、竞业限制补偿等。后众某公司就部分员工离职后跳槽至竞争对手公司，侵害其商业秘密的行为提起诉讼。法院经审理认定众某公司通过竞业限制协议等方式对相关经营信息采取有效的保密措施，符合商业秘密的构成要件。[23]

答：竞业限制协议对员工离职后加强商业秘密保护具有重要的作用，是企业用于证明已经实施保密措施，并基于此限制劳动者择业范围，避免商业秘密泄露风险的重要方式。在竞业限制的设定上，应

23. 参见上海市松江区人民法院（2024）沪0117民初401号民事判决书。

注意以下方面：

（1）竞业限制的主体应为“负有保密义务的劳动者”，企业只能与知悉商业秘密的高级管理人员、高级技术人员和其他负有保密义务的人员签订竞业限制协议，避免竞业限制主体泛化，影响一般劳动者的择业自由；

（2）竞业限制的范围、地域、期限应当与商业秘密的性质、范围、存续周期及企业实际经营需要相匹配，避免无限扩大保护范围；

（3）企业必须在竞业限制期限内按月向劳动者支付经济补偿，月补偿标准一般不低于劳动者离职前12个月平均工资的30%，且不得低于当地最低工资标准；竞业限制期限超过1年的，月补偿标准一般不宜低于员工离职前12个月平均工资的50%；

（4）竞业限制开始前，可通过向员工发送《竞业限制开始通知书》提示离职员工遵守竞业限制协议，并按约向离职员工支付经济补偿。

问23：如何履行竞业限制协议？

答：企业在履行竞业限制协议时，应当严格依照法律规定和竞业限制协议的约定，履行其应尽义务，保障劳动者的生存权利，也避免因履行瑕疵导致合同解除，无法实现商业秘密保护的目的，具体应注意以下几个方面：

（1）企业必须在竞业限制期限内按月向劳动者支付经济补偿，月补偿标准一般不低于劳动者离职前12个月平均工资的30%，且不得低于当地最低工资标准；因用人单位的原因导致三个月未支付经济补偿，劳动者可以请求解除竞业限制约定；

（2）在竞业限制期限内，企业可以基于经营需要和商业秘密保护变化，请求解除竞业限制协议，但在解除竞业限制协议时，应额外支付劳动者三个月的竞业限制经济补偿；

（3）劳动者违反竞业限制的约定，向签订竞业限制协议的企业支付违约金后，该企业可以请求劳动者按照约定返还已经支付的经济补偿并按照约定

继续履行竞业限制义务。

问24：如何加强离职员工的商业秘密管理？

答：离职员工是企业商业秘密泄露的高危环节，企业应当加强对离职员工的商业秘密管理，采取以下管理措施：

（1）开展离职谈话与保密提醒。企业应安排专人与离职员工进行离职面谈并做好面谈记录，明确告知涉密人员离职后负有的保密义务及违反保密义务的法律责任。同时，可要求离职员工签署《离职保密承诺书》，以书面形式明确保密范围、期限及违约责任，起到警示及约束作用；

（2）加强涉密载体及涉密权限管理。制定“离

职员工工作交接清单”，安排专人监督并逐项核对回收涉密载体，交接内容包括但不限于纸质文件、工作电脑、工作手机、门禁钥匙等实物，以及系统账号、密码、电子数据及载体，同时企业应当收回涉密离职员工在域名、应用系统、网络系统、门禁系统等所有内部平台的访问权限，避免离职后仍能登录；

（3）实行离职前涉密行为审查。对离职员工负责的涉密信息进行专项审查，重点排查一定期限内对商业秘密的查阅、使用情况是否存在异常，是否存在不当之处；

（4）强化脱密期管理及竞业限制评估。对涉密岗位的员工，采取脱密期管理，明确员工在脱密期内继续履行保密义务。根据员工涉密程度，评估确定是否通过竞业限制协议强化商业秘密管理。

【温馨提示】有效构建商业秘密保护体系，不仅需要司法作为“最后一道防线”的后端防护，更需要企业完善保密措施、搭建前瞻性的保密制度，才能多方位保护企业商业秘密，提升创新保护实

效。一方面，企业应当精准评估、确定秘点信息，对秘点信息采取行之有效的保密措施。另一方面，通过强化保密教育、制定保密制度、加强员工入职、离职的商业秘密管理，设立有效的商业秘密“防火墙”，从而避免商业秘密泄露。


云间·山中竹
YUNJIAN SHANZHONGZHU
法官秘谈—商业秘密保护
松法系列微课程
第一讲
第二讲
第三讲
第四讲
第五讲
第六讲
请扫码观看