



企业知识产权法律 保护指引手册

Guidelines for Legal Protection of
Corporate Ips



上海检察机关知识产权保护研究中心
Research Center for Intellectual Property Protection of Shanghai Procuratorial Organs

上海市人民检察院第三分院
Third Branch of Shanghai People's Procuratorate

2024年4月



企业知识产权合规管理提示

1. 什么是知识产权合规风险

知识产权合规风险，是指企业及其员工因知识产权不合规行为，引发法律责任，造成刑事责任、经济或声誉损失以及其他负面影响。

2. 企业知识产权合规管理的目的

通过对知识产权合规风险的有效识别和管理，确保公司管理和各项经营活动的合法合规，推动企业全面加强知识产权合规管理，提升依法合规经营管理水平，保持企业持续健康发展。

3. 如何建设企业知识产权合规体系

企业应建立健全知识产权合规体系，涵盖组织体系、制度体系、运行体系、风险识别预警、合规文化培育等。

【组织体系】可根据自身行业性质、经营规模等合理选择和设置知识产权合规部门或合规人员，组织、协调和监督合规管理工作，在直接负责各项合规管理工作的同时为其他部门提供合规管理支持，并确保其对涉及重大合规风险事项的一票否决权。

【制度体系】建立健全规范化的知识产权事务管理和决策流程，将知识产权合规审查作为制度制定、重大事项决策、重要合同签订、重大项

目运营等经营管理行为的必经程序，及时对不合规的内容提出修改建议，未经合规审查不得实施。企业应建立健全合规监察、合规举报、绩效评价、不合规调查、文件信息化管理、保密管理等制度。

【运行体系】注意合规管理运行体系建设，包含获取合规、维护合规、运用合规。

(1) 获取合规。应及时申请注册登记各类知识产权、明确有关专利申请、集成电路布图设计登记、商标注册、著作权登记、商业秘密保护等知识产权获取及其后续维护或主动放弃的管理措施和工作程序。

(2) 维护合规。应明细处置和运营知识产权管理规定，明确职务发明成果的界定条件以及委托或合作开发成果知识产权归属的处置原则，明确有关专利权、商标权、著作权等知识产权转让、许可、投资、质押的管理措施和工作程序。

(3) 运用合规。企业应注重生产经营环节知识产权管理，明确在原材料及设备采购（包括软件等）、技术和产品开发、技术转让（许可）与合作、委托加工、产品销售、广告宣传或展销、招投标、进出口贸易、企业合资及并购和上市等环节中可能涉及的各类知识产权事务的管理措施和工作程序。

【风险识别预警】

通过完善合规风险信息收集机制，全面系统

梳理企业经营活动中可能存在的合规风险，建立合规风险台账，对风险源、风险类别、风险形成因素、可能发生的后果及发生的概率等展开系统分析，对有典型意义、普遍存在的以及可能造成严重后果的风险应及时发布预警。

【合规文化培育】

建立对技术人员、知识产权管理人员、全体员工分层级合规培训制度。从增强知识产权意识、知识产权价值观、营造崇尚创新尊重知识产权的氛围、重视知识产权宣传教育等方式进行知识产权文化的建设。结合知识产权管理制度和人才建设，构建有利于调动企业员工知识产权工作积极性的激励机制，树立尊重和保护知识产权的企业形象。

企业知识产权全流程保护攻略

【企业篇】

随着我国经济步入高质量发展阶段，知识产权对于企业的创新、竞争与可持续发展起到越发重要的引领作用。知识产权的管理与保护贯穿企业经营的全过程、各环节，企业需结合自身的业务特点、经营规模、发展规划等情况采取高效合理的保护措施，健全内部知识产权合规管理体系，强化外部知识产权风险防范能力。

1. 知识产权的创造

企业应根据自身业务特点、目标市场等因素定位核心技术、主要品牌等，制定与企业发展策略相适应知识产权布局规划。对于品牌培育，企业应采取“商标先行”的策略，及时确定业务领域并注册商标，以免遭到他人抢注。对于研发成果，企业可视技术的创新性及价值性进行分层级、分类别的专利布局，根据技术类型在专利、著作权、商业秘密中合理选择单一保护模式或交叉保护模式。

企业在申请和注册前应进行充分的检索和审核，或委托信用良好的专业知识产权代理机构代为申请注册，避免出现不符合申请条件、侵犯他人在先权利等情况。同时，企业须注意妥善保存知识产权权

利证书、缴费记录、研发记录、著作权原始载体等能够用于佐证权属的文件资料。

2. 知识产权的运用

企业应合理、规范运用知识产权。例如，在使用注册商标的过程中不得连续三年怠于使用或擅自对商标进行拆分、组合、增加元素等改变，否则将面临被撤销或侵权的风险；将知识产权转让或许可他人使用时，可以对许可使用中的增值部分进行预先评估或约定权属，要求相关方履行审查、备案或登记程序；当企业发展到一定阶段，需要进一步扩张知识产权版图时，可以通过 PCT 申请的方式对专利进行海外布局，或综合考虑收购方向、专利有效期、专利许可情况等因素进行专利收购。

3. 知识产权的管理

有条件的企业可以通过建立知识产权数据库等方式对所述产业领域的知识产权信息及企业持有的知识产权权利状况、运行状况进行梳理汇总并及时更新、维护、研判，适时调整知识产权管理策略。一要强化涉知识产权合同管理。如在委托开发、委托加工、贴牌生产等合同中应明确保密义务、知识产权权属、许可使用范围、侵权责任承担等内容；二要强化经营活动中的知识产权审查。如在进货时应对供货商授权许可文件、经营资质进行核实，拒绝购进明显低于市场价、缺少质量合格证等异常产品，同时保留购货合同、票据、汇款单等证明货物合法来源的证据。

4. 知识产权的保护

企业应构建覆盖事前预警、事中管控、事后反馈的知识产权风险管理体系，根据风险发生的时间、频次、影响对知识产权风险进行分级分类，及时制定防范与应对预案。如企业持有商业秘密，还应进一步根据企业规模、商业秘密的价值及保护需求等对涉密人员、涉密载体、涉密场所、涉密信息采取相应的保密措施。如企业知识产权遭到侵犯，可以根据侵权行为类型、受损程度等情况合理运用行政保护、刑事保护、民事保护等多种救济渠道。企业应及时自行依法取证或申请公证取证，或通过向法院申请证据保全、诉前禁令等形式防止证据灭失，限制损害扩大。

【员工篇】

员工是企业发展和创新创造的动力来源，但因员工入职、离职而引发的知识产权纠纷也层出不穷。为保护自身合法权益，避免陷入不必要的法律纠纷，员工应擦亮双眼，强化知识产权法律意识，牢牢把握入职、在职、离职三阶段的风险识别与防控。

1. 入职阶段

员工在入职前，应当仔细阅看劳动合同中约定的保密条款，着重了解企业约定的保密信息范围、保密期限、员工接触及使用商业秘密的方式和权限等。如入职的企业与原公司存在竞争关系或者研发成果存在关联，员工应当避免使用他人的商业秘密。

为保障自身合法权益，建议员工与企业明确约

定职务作品、职务发明的归属及相关奖励报酬制度。不同身份和职务的员工可以区分不同情形与企业约定职务作品、职务发明权属：如对于一般研发人员，职务发明归属于企业但是研发人员有优先受让权；对于技术入股的股东、高管，应分别明确初代技术和迭代技术的权属。员工在职务范围以外创作的作品或研发的技术，企业应在员工同意后使用，使用费依双方约定确定。

2. 在职阶段

员工在职期间应认真参与企业组织的各项知识产权培训及考试，详细了解并遵守企业的知识产权保护制度，准确识别、规范使用企业享有知识产权的无形资产，谨慎使用带有保密标记或采用特殊方式管控的纸质文件或电子文档等信息载体。

在开展商业合作、技术合作、跨境合作等业务活动的过程中，员工如因业务需要向外部人员或者企业提供涉密信息，则应提醒企业与外部人员或者企业签订保密协议；如因工作需要参加职务相关的技术交流会或对外发布可能涉及保密信息的内容时，应交由保密负责人在参与交流或发布信息前进行保密审查。

3. 离职阶段

正式离职前，员工应配合企业完成与保密义务有关的各项流程和手续，包括配合企业对涉密设备、涉密文件资料及其他相关物品进行清查盘点，按要求返还、销毁并做好台账登记，向有关客户、供应商、

合作单位等告知离职事宜并做好交接工作等。

在原企业担任高级管理人员、高级技术人员和负有保密义务的员工可能与企业签署竞业限制协议，员工在离职前应再次向企业确认离职后竞业限制协议是否生效，如果生效，则应关注竞业限制协议约定的竞业限制范围、地域、期限、违约责任以及经济补偿金额等具体事项。未签署竞业限制协议或竞业限制期限届满的离职员工，如在与原企业有竞争关系的企业任职，或从事同类业务的，不得使用原任职企业的涉密信息、高薪挖角原企业员工以获取涉密信息或者利用在原企业的人脉关系唆使、利诱他人协助获取涉密信息。

企业知识产权保护状况自查表

	问 题	是	否
1	企业是否具有明确的知识产权管理保护制度？是否形成规范性文件？		
2	企业对没达到申请水平的发明、商业秘密是否有明确的管理保护机制？		
3	企业是否针对技术开发部门设置网络化的知识产权信息管理系统？		
4	申请知识产权前，企业是否要求相关人员检索现有技术或者先有权利情况？		
5	企业在产业化和销售产品之前是否开展知识产权调查，以避免侵权纠纷？		
6	企业在技术开发阶段至产业化阶段每个阶段是否明确知识产权法律风险责任人？		
7	企业是否与员工就本企业知识产权保护而签订竞业禁止协议或者保密协议？		
8	企业是否就技术开发人员创造的知识产权归属与技术人员签订相关协议，明确权属？		
9	企业是否主动对使用的商标申请注册，或对创造的著作权、集成电路布图设计进行权属登记？		
10	企业在面临自有知识产权被侵权的情况，是否主动收集相关被侵权线索、证据，并提交司法机关？		

Tips for Corporate IP Compliance Management

1. Concept of IP compliance risk

Intellectual property (IP) compliance risk refer to a company's possible exposure to legal liability, criminal liability, economic or reputational loss, and other negative impacts resulting from the non-compliant IP-related behaviors of the company and its employees.

2. Purpose of corporate IP compliance management

Corporate IP compliance management is performed based on the effective identification and management of IP compliance risks to ensure that the management and business activities of companies are lawful, urge companies to comprehensively strengthen their IP compliance management work, improve their lawful operation and management levels, and maintain their sustainable and healthy development.

3. How to build IP compliance management systems

Companies should build and improve their IP compliance management systems, including the organizational system, institutional system, operation system, risk identification and early warning system, and compliance culture cultivation system.

[Organizational System] Companies may reasonably select and appoint an IP compliance management department or personnel based on their industry characteristics and business scale to organize, coordinate, and supervise IP compliance management work, and provide compliance management support for other departments while directly carrying out various compliance management work. Companies shall ensure that the IP compliance management department or personnel has the veto power on matters involving major compliance risks.

[Institutional System] Companies shall establish and improve a standardized IP affairs management and decision-making process and take IP compliance review as a compulsory procedure for business management activities such as formulation of rules and regulations, decision-making on major matters, signing of important contracts, and operation of major projects; promptly provide rectification suggestions for non-compliant matters and ensure that the preceding activities will not be implemented before passing the IP compliance view. Companies should establish and improve rules and regulations for compliance supervision, compliance reporting, performance evaluation, non-compliance investigation, documented information management, confidentiality management, etc.

[Operating System] Companies should attach

importance to the construction of a compliance management operating system to ensure compliance in IP acquisition, maintenance, and use.

(1) Compliance in acquisition. Companies shall make timely applications for the registration of various types of IPs and establish clear management measures and working procedures regarding the acquisition of IPs such as the patent applications, registrations of integrated circuit layout designs, trademarks, and copyrights, and trade secret protection, as well as their subsequent maintenance or voluntary waiver.

(2) Compliance in maintenance. Companies shall develop detailed rules for the disposal and operation of IPs, specify the conditions for defining service inventions and the principles for determining the ownership of IPs in commissioned work or co-authored work, and establish management measures and working procedures for the transfer, licensing, investment, and pledge of IPs such as patents, trademarks, and copyrights.

(3) Compliance in use. Companies should pay attention to the management of IPs in the processes of production and operation and establish management measures and working procedures for various IP affairs that may be involved in the procurement of raw materials and equipment (including software), technology and product development, technology transfer (licensing) and cooperation, commissioned processing, sales of products,


advertising or sales exhibitions, tendering and bidding, import and export trade, joint ventures, mergers and acquisitions, and listing.

[Risk Identification and Early Warning]

Companies shall improve the compliance risk collection mechanism, comprehensively and systematically sort out compliance risks that may exist in business activities, and build a compliance risk ledger to systematically analyze risk sources, risk categories, risk formation factors, possible consequences, and the likelihood of occurrence; and promptly issue early warnings for risks that are of typical significance, widespread, and likely to cause serious consequences.

[Compliance Culture Cultivation]

Companies shall establish a hierarchical compliance training system for technicians, IP management employees, and all employees; and cultivate IP culture by enhancing IP awareness and IP values, creating an atmosphere of advocating innovation and respecting IP, and attaching importance to IP publicity and education. Based on the development the IP management regulations and the cultivation of IP compliance talents, companies shall establish an incentive mechanism that is conducive to increasing the employees' enthusiasm for IP compliance work and build a corporate image that respects and protects IPs.



Guidelines for the Whole- Process Protection of Corporate IPs

[Companies]

As China's economy enters a stage of high-quality development, IPs play an increasingly important role in driving the innovation, competition, and sustainable development of companies. Companies shall manage and protect their IPs throughout the entire process and every link of their business operations. They shall take efficient and reasonable protection measures based on their business characteristics, operating scale, and development plans, improve their internal IP compliance management systems, and strengthen external IP risk prevention capabilities.

1. Creation of IPs

Companies shall develop core technologies and main brands based on factors such as their business characteristics and target markets and make IP deployment plans that match their development strategies. In terms of brand cultivation, companies shall adopt a strategy of "trademark first". They should promptly determine the business areas and register their trademarks as soon as possible to prevent others from

registering them in bad faith. For R&D results, companies can deploy hierarchical and categorized patents based on the innovativeness and value of the technology and reasonably choose a single or comprehensive IP protection model among patents, copyrights, and trade secrets according to the type of technology.

Before applying for IP registration, companies should conduct sufficient retrieval and reviews or engage a reputable professional IP agency to apply for IP registration on their behalf to avoid non-compliance with the application conditions or infringement upon the prior rights of others. In addition, companies should properly keep documents that can be used to prove their ownership of IPs, such as IP rights certificates, payment records, R&D records, and original copyright carriers.

2. Use of IPs

Companies should use IPs in a reasonable and standardized manner. For example, after registering a trademark, companies must use it at least once within three consecutive years and must not make unauthorized changes to the trademark such as splitting it, combining it with other trademarks, or adding elements to it. Otherwise, they may be exposed to risks such as trademark revocation or infringement. When transferring or licensing IPs to others, companies may pre-evaluate the value-added part of the licensed IPs, or agree on

the ownership thereof with the transferee or licensee, and require the transferee or licensee to perform review, filing, or registration procedures. When a company develops to a certain stage and needs to further expand its IP layout, it may file applications for PCT patents to deploy patents abroad, or buy patents taking into account factors such as the acquisition direction, patent validity period, and patent licensing status.

3. Management of IPs

Where possible, companies may take measures such as building an IP database to sort out, summarize, update, maintain, and analyze IP information in their industrial areas, the IP rights held by them and their operation status, to adjust their IP management strategies as needed. First, strengthen the management of IP-related contracts. For example, in contracts such as commissioned development, commissioned processing, and OEM contracts, companies shall specify the confidentiality obligations, IP ownership, license scope, liabilities for infringement, and other relevant content. Second, strengthen the IP review in business activities. For example, when purchasing products, companies should verify suppliers' authorization and licensing documents and business qualifications, reject abnormal products such as those that are priced significantly lower than the market price or lack quality certificates, and

keep the evidence that can prove the legal source of the products, such as the purchase contracts, bills, and remittance orders.

4. Protection of IPs

Companies shall build an IP risk management system that covers pre-event early warning, in-process control, and post-event feedback, classify IP risks based on the occurrence time, frequency, and impact, and promptly develop prevention and response plans. For companies that hold trade secrets, they shall also take confidentiality measures for the staff, carriers, locations, and information involved in the trade secrets based on their business scale, the value of the trade secrets, and the protection requirements. If a company's IP is infringed, the company can turn to a variety of reliefs such as administrative protection, criminal protection, and civil protection based on factors such as the type of infringement and degree of damage. In addition, the company shall, in accordance with the law, promptly take measures such as collecting evidence on their own, applying for notarization of the evidence-collecting process, or applying to the court for evidence preservation or pre-litigation injunction to prevent the loss of evidence and further damage.

[Employees]

Employees are the driving force for companies to develop, innovate, and create values. However, many IP-related disputes arise from employees' on-boarding and separation. To protect their legitimate rights and interests and avoid unnecessary legal disputes, employees should keep their eyes open, strengthen their legal awareness of IPs, and identify and prevent IP-related risks in the on-boarding, in-service, and separation stages.

1. On-boarding stage

Before joining a company, employees should carefully read the confidentiality clauses stipulated in the employment contract and focus on such matters as the scope of confidential information, the confidentiality period, and the methods and permissions for employees to access and use trade secrets. If the company that an employee is about to join is in competition with the employee's former employer or their R&D results are related, the employee should avoid using the trade secrets of the former employer.

To protect the legitimate rights and interests of employees, it is recommended that employees and the employer clearly agree on the ownership of service works and inventions and the related reward and compensation rules. The ownership of service works and inventions between employees and an employer can be determined

based on the roles and positions of the employees. For example, if the employee is a general researcher, the service inventions developed by the employee shall be owned by the employer but the employee shall have the right of first refusal for future transfer of the inventions. If the employee is a shareholder or a senior executive who invests in the company using technology, the employee and the company shall clarify the ownership of the first-generation technology and its iterations, respectively. To use works or technology created or developed by employees beyond their duties, the employer shall obtain consent from the employees and make compensation to the employees in the agreed amount.

2. In-service stage

During their employment, employees should take various IP-related training and examinations organized by the employer, understand and comply with the employer's IP protection regulations, accurately identify and properly use intangible assets whose IPs belong to the employer, and take cautions when using information carriers such as paper or electronic documents that are marked as confidential or managed in a special manner.

Where an employee needs to provide confidential information to external individuals or companies for the purpose of carrying out business activities such as

business cooperation, technical operation, or cross-border cooperation, the employee shall request the employer to sign a non-disclosure agreement (NDA) with these external individuals or companies. Where an employee needs to participate in a job-related technical seminar or publicly disclose any content that may involve confidential information for work reasons, the employee shall be reviewed for confidentiality purpose by the person in charge of confidentiality work before his/her participation in the technical seminar or disclosure of relevant content.

3. Separation stage

Before formally leaving a company, an employee shall cooperate with the company in completing various processes and procedures required for fulfilling their confidentiality obligations, such as cooperating with the company in conducting an inventory of devices and documents containing confidential information and other relevant items, returning or destroying these items as required, creating a ledger to record the returned or destroyed items, notifying the related clients, suppliers, and partners of the separation, and carrying out the handover.

Employees who serve as senior managers or senior technicians or have confidentiality obligations in a company may have signed a non-competition agreement

with the company. Before leaving the company, they should confirm with the company again whether the non-competition agreement takes effect after their separation. If yes, they should pay attention to specific matters such as the scope, territory, and duration of non-competition, liabilities for breach, and amount of economic compensation specified in the non-competition agreement. For employees who have not signed a non-competition agreement or those whose non-competition agreement has expired, if they join a company that competes with their former employer or is engaged in the similar business as that of their former employer, they are not allowed to use the confidential information of their former employer, hire employees of the former employer with high salaries for the purpose of obtaining confidential information of their former employer, or use personal connections to incite or induce others to assist in obtaining confidential information of their former employer.

Self-Checklist for Corporate IP Protection

	Question	Yes	No
1	Does your company have a clear IP management and protection system? Does your company have normative documents for IP protection?		
2	Does your company have a clear management and protection mechanism for inventions and trade secrets that do not meet the application requirements?		
3	Does your company have a network-based IP information management system for the technology development department?		
4	Before applying for IP registration, does your company require the relevant personnel to search for existing technology or prior rights?		
5	Does your company conduct IP investigations before producing and selling products to avoid infringement disputes?		
6	Does your company clearly identify the persons responsible for IP-related legal risks at each stage from technology development to mass production?		
7	Does your company sign a non-competition agreement or NDA with employees regarding IP protection?		
8	Does your company sign relevant agreements with technical developers to clarify the ownership of IPs created by technical developers?		
9	Does your company proactively apply for registration of the trademarks used or register the ownership of the copyrights or integrated circuit layout designs created?		
10	In case of infringement of your company's IP, does your company proactively collect the relevant clues and evidence of the infringement and submit them to judicial authorities?		