

陕西省市场监督管理局

通告

陕市监通告〔2026〕40号

陕西省市场监督管理局 关于印发《陕西省企业商业秘密保护 合规指引》的通告

为助力提升经营者商业秘密保护能力，根据《中华人民共和国反不正当竞争法》及相关法律法规，结合执法实践和监管实际，我局制定了《陕西省企业商业秘密保护合规指引》，现通告如下。



陕西省企业商业秘密保护合规指引

第一章 总则

第一条【制定目的】

为加强企业商业秘密保护工作，规范商业秘密管理行为，防范商业秘密泄露和侵权风险，维护企业合法竞争优势，保障企业持续创新能力和市场竞争力，服务新质生产力发展与高水平科技自立自强，根据《中华人民共和国反不正当竞争法》《中华人民共和国民法典》《中华人民共和国劳动合同法》《商业秘密保护规定》等相关法律法规和司法解释，结合企业经营管理实际，制定本指引。

本指引旨在建立覆盖商业秘密识别、分类、使用、流转、存储、退出及维权处置全过程的合规体系，实现商业秘密保护工作的制度化、规范化、体系化与数字化。

第二条【适用范围】

本指引适用于全省企业各部门、分支机构、员工以及参与企业研发、生产、经营活动的合作单位、劳务派遣人员、实习生、顾问及其他相关主体。

涉及企业商业秘密管理、使用、接触、传输、保存和处置的全部业务活动，均应遵守本指引。

第三条【商业秘密定义】

本指引所称商业秘密，是指不为公众所知悉、具有商业价值并经企业采取相应保密措施的技术信息、经营信息等商业信息。

商业秘密的认定应同时符合以下条件：

（一）秘密性：相关信息在涉嫌侵权行为发生时，未进入公开领域，无法通过合法公开渠道直接获得。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，符合秘密性条件的，仍可认定为商业秘密。

（二）价值性：相关信息具有现实的或者潜在的商业价值，能够为企业带来资产增加、营业收入或利润增长、用户数量增长、成本费用降低、研发时间缩短、交易机会增加、商业信誉或商品声誉提升等商业利益或竞争优势。生产经营活动中形成的阶段性成果或失败的实验数据、技术方案，符合条件的，一并受本指引保护。

（三）保密性：企业已经根据商业秘密性质、价值程度、载体形式以及管理需要，采取与商业秘密及其载体的性质、商业价值等因素相适应的合理保密措施。

第四条【保护基本原则】

企业商业秘密保护工作遵循以下原则：

（一）合法合规原则：商业秘密管理活动应符合国家法律法规要求，不得通过违法方式获取、利用或者保护商业信息，不得滥用商业秘密制度排除、限制竞争或不当限制员工职业自由。

（二）限制知悉原则：商业秘密仅向因工作需要确需知悉的人员开放，实行最小授权与最小必要原则。

（三）分级分类原则：根据商业秘密价值程度、泄露风险和影响范围实行分类分级管理，确定不同密级、保密期限和知悉范围。

（四）全过程管理原则：商业秘密保护贯穿信息形成、使用、流转、保存和销毁全生命周期。

（五）预防为先原则：通过制度建设、技术措施和人员管理降低商业秘密泄露风险，建立事前防范、事中控制、事后救济的闭环管理机制。

（六）权利平衡原则：在保护企业商业秘密的同时，尊重员工正当职业权利与个人信息权益，保密措施与竞业限制应符合比例原则，不得过度限制员工职业技能与择业自由。

（七）多元共治原则：建立企业自治、行政保护、司法救济、行业自律相结合的多元保护格局。

第二章 商业秘密识别与分类管理

第五条【识别范围】

企业商业秘密主要包括以下内容：

（一）技术信息：包括但不限于产品设计方案、技术研发资料、工艺流程、配方及生产参数、实验数据（含失败实验数据）、算法

模型、计算机程序及代码、软件源代码、技术图纸、样品样机信息、未公开专利申请信息、数据集合等。

（二）经营信息：包括但不限于客户名单及客户交易习惯、意向、内容等深度信息，供应商信息，商业合作方案，招投标文件，营销策略，产品定价方案，财务数据，投融资计划，采购渠道，市场分析报告，管理诀窍等。

（三）其他商业信息：企业认为符合商业秘密构成条件的其他信息。

第六条【分级管理】

企业根据商业秘密的重要程度和泄露风险，将商业秘密划分为：

（一）核心商业秘密：指对企业持续发展、市场竞争优势具有决定性影响的信息。泄露可能导致企业遭受重大经济损失或竞争优势丧失。如核心技术方案、关键算法、未公开战略规划、重大投融资决策等。

（二）重要商业秘密：指对企业经营活动和竞争优势具有重要影响的信息。如重要客户资料、供应链信息、经营策略、阶段性研发成果等。

（三）一般商业秘密：指对企业经营具有一定价值的信息。如一般业务资料、内部管理文件、普通技术改进等。

企业应对不同密级的商业秘密设定不同的保密期限、知悉范围、审批权限和技术防护措施，并在载体上作出明显密级标识。

第七条【商业秘密清单管理】

企业应建立商业秘密清单（目录）动态管理制度，明确商业秘密的名称、密级、责任部门、责任人、形成时间、保密期限、知悉范围、载体形式及存储位置。清单应定期更新，至少每年复核一次。

第三章 商业秘密管理组织与职责

第八条【管理机构设置】

企业应建立商业秘密保护管理组织体系：

- （一）企业主要负责人承担商业秘密保护工作的总体责任；
- （二）设立商业秘密保护委员会或指定首席合规官统筹商业秘密保护工作；
- （三）设立专职或兼职的商业秘密管理部门；
- （四）各业务部门设立保密联络员，形成纵向到底、横向到边的管理网络。

第九条【管理职责】

商业秘密保护部门主要职责：

- （一）制定、修订商业秘密保护制度及操作规程；
- （二）建立并维护商业秘密清单；
- （三）组织保密培训与合规文化建设；
- （四）开展风险评估与合规审计；
- （五）处理泄密事件及维权事务；

(六) 监督第三方合作中的保密义务履行;

(七) 建立举报与吹哨人保护机制。

业务部门职责:

(一) 识别、申报本部门商业秘密;

(二) 落实本部门保密措施与权限管理;

(三) 管理本部门涉密人员及第三方接触人员;

(四) 及时报告泄密风险与异常访问行为。

第四章 商业秘密生命周期管理

第十条【形成阶段保护】

企业在研发、经营活动中形成商业秘密时,应及时:

(一) 确认信息属性,评估是否符合商业秘密构成要件;

(二) 确定责任部门与责任人;

(三) 登记商业秘密目录,明确密级与保密期限;

(四) 采取相应保密措施后方可允许人员接触。

第十一条【使用阶段保护】

员工使用商业秘密时,应遵守:

(一) 授权访问制度,按密级与岗位权限访问;

(二) 最小必要原则,仅获取完成工作所必需的信息;

(三) 禁止超范围使用、复制、拍摄、截屏、录屏;

（四）核心商业秘密原则上不得在无监控的私人设备或公共网络环境中处理。

第十二条【流转阶段保护】

商业秘密内部流转应：

- （一）记录流转人员、时间、内容、用途；
- （二）限定使用范围与二次传播权限；
- （三）保存流转记录备查；
- （四）采取必要技术保护措施。

对于电子文件、云存储、邮件传输、即时通讯、远程办公等方式，应采取权限控制、身份认证、数据脱敏、操作日志留痕、访问记录等措施。禁止未经授权将商业秘密传输至不受企业控制的电子邮箱、云盘、网络存储空间或电子设备。

第十三条【保存与销毁管理】

商业秘密载体包括：

- （一）纸质文件；
- （二）电子文件及数据库；
- （三）样品样机；
- （四）声像资料；
- （五）其他承载商业秘密的信息载体。

保存要求：核心商业秘密应实行物理隔离与加密存储，重要商业秘密应定期备份，一般商业秘密应分类归档。

销毁要求：销毁涉密资料应履行审批登记程序，采取粉碎、焚毁、不可恢复的数据擦除等方式处理，确保信息不可复原。销毁过程应由双人监销并留存记录。

第十四条【数字化与跨境场景保护】

针对远程办公、跨境协作、云服务、人工智能训练数据等场景，企业应采取：

- （一）零信任架构下的权限分级与动态授权；
- （二）数据脱敏、加密传输、终端安全检测；
- （三）跨境数据传输前的合规审查，确保符合数据出境安全评估要求；
- （四）对境外服务器、云端存储的访问日志进行留痕与审计。

第五章 涉密人员管理

第十五条【入职管理】

（一）对新入职员工进行背景调查，评估其与前雇主的保密义务及竞业限制义务冲突风险；

（二）在劳动合同或保密协议中明确保密范围、期限、义务及违约责任；

（三）对核心岗位人员，应在入职前明确告知其岗位涉密性质及相应权利义务。

第十六条【员工保密义务】

企业应与涉密员工签订保密协议。保密协议至少包括：

- （一）保密范围与密级划分；
- （二）保密期限（一般为长期，直至该信息进入公有领域）；
- （三）保密义务的具体行为要求；
- （四）违约责任与救济方式；
- （五）争议解决条款。

保密协议应遵循公平原则，不得将已进入公有领域的信息、员工个人知识经验或职业技能纳入保密范围，不得不当限制员工正当择业权利。

第十七条【在职人员管理】

（一）定期开展保密培训，培训内容应包括商业秘密认定标准、泄密风险、员工保密义务、违法责任及权利救济途径；

（二）对核心涉密人员实行分区管理、门禁控制、专用设备配置；

（三）建立异常行为监测机制，对批量下载、非工作时间访问、异常外发等行为进行预警；

（四）员工岗位调整时，应及时调整其访问权限，实行权限回收与重新授权。

第十八条【离职人员管理】

员工离职时，企业应：

（一）进行离职面谈，书面告知其离职后继续承担的保密义务及竞业限制义务（如有）；

（二）回收涉密资料、样品、存储介质及门禁卡等；

（三）监督删除或返还其私人设备中保存的涉密信息；

（四）解除或调整其信息系统访问权限；

（五）完成工作交接并签署离职交接清单，清单应载明已返还或清除的涉密载体明细；

（六）对核心涉密人员，企业可依据《劳动合同法》在劳动合同或保密协议中约定竞业限制条款。在员工离职时，企业如需对其实行竞业限制，应在离职前书面告知，明确竞业限制的范围、地域、期限及经济补偿标准。

第十九条【竞业限制管理】

企业与员工约定竞业限制的，应遵守：

（一）限于高级管理人员、高级技术人员和其他负有保密义务的人员；

（二）竞业限制期限不得超过二年；

（三）在竞业限制期限内按月给予员工经济补偿，补偿标准应符合地方规定或双方约定，不得低于法定最低标准；

（四）竞业限制范围应明确、合理，限于与本企业有竞争关系的同类业务企业，不得过度扩大；

（五）企业未按约定支付经济补偿达一定期限的，员工有权请求解除竞业限制协议；

（六）竞业限制协议不得排除员工在限制期满后使用其个人知识经验的权利。

保密义务与竞业限制义务为相互独立的法律义务，保密义务不因竞业限制期限届满而终止；竞业限制期限届满后，员工仍应依法承担保密义务，但有权在竞争企业从事不涉及泄露原企业商业秘密的工作。

第六章 第三方合作与跨境合规

第二十条【合作信息披露原则】

企业开展合作活动时，应遵循“必要披露、限定用途、全过程控制”原则。不得向合作方提供超出合作目的范围的信息。

第二十一条【合同保护机制】

企业与外部主体合作时，应签订保密协议或设置保密条款。主要包括：

- （一）商业秘密范围及密级；
- （二）使用目的与使用方式；
- （三）保密期限；
- （四）禁止披露、反向工程及分许可义务；
- （五）合作终止后的信息返还、销毁与清除义务；

(六) 违约责任与争议解决。

第二十二条【供应链与开源合规】

(一) 对供应商、承包商、咨询机构等第三方进行保密资质审查；

(二) 在供应链合作中建立分级授权与信息隔离机制；

(三) 使用开源软件、第三方代码时，应评估其许可证对商业秘密的影响，避免强制披露要求；

(四) 对受托加工的技术资料实行单向输出与回收确认。

第二十三条【域外与跨境保护】

(一) 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，企业可依法请求境内有关部门处理；

(二) 涉及跨境数据流动的，应遵守《数据出境安全评估办法》等规定，事前开展安全评估与合规审查；

(三) 在境外参展、销售、投资时，应提前进行商业秘密侵权风险排查与专利自由实施分析。

第七章 泄密风险处置与多元救济

第二十四条【侵犯商业秘密行为】

商业秘密侵权行为是未经商业秘密权利人许可，直接或间接获取、披露、使用或许可他人使用商业秘密，使得商业秘密权利人遭受损失的行为。

侵犯商业秘密的行为体现为下列情形：

（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；

（五）第三人明知或者应知商业秘密权利人的员工、前员工或者其他企业、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。

第二十五条【泄密事件报告】

发现商业秘密侵权行为或泄密事件时，应立即向商业秘密管理部门报告。报告内容应包括：涉事人员、涉事信息、发现时间、可能范围、初步证据等。

第二十六条【应急处置措施】

企业应立即采取以下措施：

（一）停止信息扩散，限制涉事人员对相关系统、设备及信息的访问权限，对设施系统、设备采取技术隔离措施；

（二）保存电子数据，固定访问日志、邮件记录、传输记录等电子证据；

（三）对涉事场所、设备进行封存或拍照录像；

（四）开展内部调查，查明泄密途径与责任人员；

（五）评估损失与影响，制定补救方案；

（六）必要时向公安机关报案或向市场监督管理部门投诉。

鼓励采用区块链存证、时间戳、电子数据保全等方式固定证据。

第二十七条【维权路径与民行刑衔接】

商业秘密受到侵犯时，企业可以依法采取以下一种或多种救济措施：

（一）协商调解：与侵权方协商，要求其停止侵权、返还或销毁载体、赔偿损失；

（二）行政投诉：向市场监督管理部门投诉，请求责令停止违法行为、没收违法所得并处以罚款（一般情节：十万元以上一百万元以下，情节严重：一百万元以上五百万元以下）；

（三）民事诉讼：向人民法院提起侵权之诉，请求停止侵害、赔偿损失、消除影响。赔偿数额按照实际损失或侵权获利确定，故意侵权且情节严重的，可适用一倍以上五倍以下惩罚性赔偿；

（四）刑事报案：对符合“情节严重”标准（如损失数额或违法所得数额三十万元以上，或两年内因侵犯商业秘密受过刑事处罚或行政处罚再次实施且数额十万元以上）的，向公安机关报案，追究其刑事责任；

（五）归入权行使：对违反忠实义务的董事、监事、高级管理人员，依据《公司法》行使归入权。

企业应建立民行刑衔接机制，民事程序中注重证据保全，为可能的行政、刑事程序预留接口。

第二十八条【举证责任与推定规则】

在商业秘密侵权纠纷中，企业应注重以下举证与抗辩规则：

（一）权利人提供初步证据证明已采取保密措施且合理表明商业秘密被侵犯的，涉嫌侵权人应证明该信息不属于商业秘密；

（二）有证据证明涉嫌侵权人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条件的，可推定侵权成立，由涉嫌侵权人证明其信息合法来源；

（三）“实质相同”的认定应综合考虑信息异同程度、所属领域相关人员是否容易想到区别、用途与使用方式差异、公有领域信息情况等因素。

第八章 监督评价与责任追究

第二十九条【保密培训制度】

企业应建立分层分类的保密培训体系：

- （一）新员工入职培训；
- （二）全员年度常规培训；
- （三）核心涉密人员专项培训；
- （四）第三方人员入场培训。

培训内容应包括：商业秘密认定标准、泄密风险识别、员工保密义务与权利、违法责任、举报渠道与吹哨人保护。

第三十条【风险检查与合规审计】

企业应定期开展：

- （一）商业秘密风险评估，识别新业务、新技术、新合作模式下的泄密风险；
- （二）权限审查与访问日志审计；
- （三）制度执行检查与整改评价；
- （四）第三方保密履约情况抽查；
- （五）合规审计报告应提交管理层并限期整改。

第三十一条【举报与吹哨人保护】

企业应建立商业秘密侵权举报机制：

- （一）设立举报渠道，保护举报人身份与信息安全；
- （二）对实名举报并经查实的，给予适当奖励；
- （三）禁止对举报人进行打击报复；

（四）举报人提供的线索符合行政或刑事立案条件的，及时移送有关部门。

第三十二条【责任追究】

违反本指引规定，造成商业秘密泄露或企业损失的，企业依法追究相关责任：

（一）对员工的处分包括：警告、降职、解除劳动合同、要求赔偿损失等；

（二）对第三方合作方的处分包括：终止合作、要求承担违约责任、追偿损失等；

（三）涉嫌违反《反不正当竞争法》的，移送市场监督管理部门；

（四）涉嫌构成犯罪的，依法移送公安机关处理。

第三十三条【合规激励】

企业应积极申请商业秘密保护示范单位、知识产权管理体系认证等，将商业秘密保护纳入企业 ESG 评价与合规管理体系。

第九章 附则

第三十四条【解释与实施】

本指引由陕西省市场监督管理局解释。

本指引自发布之日起实施。原有相关规定与本指引不一致的，以本指引为准。