淄博市市场监督管理局

关于印发《淄博市新材料产业商业秘密保护工作指引》的通知

各区县市场监管局，全市相关企业：

现将《淄博市新材料产业商业秘密保护工作指引》印发给你们，请相关企业结合经营情况，参考使用。各区县市场监管局在开展商业秘密保护行政指导时，可作为工作资料提供给企业借鉴使用。

相关企业、区县市场监管局要加强商业秘密保护，将实际工作中好的做法、经验、意见和建议，及时反馈给市市场监管局反不正当竞争科，以便进一步改进和完善。

联系人：杜道强　　联系电话：3110956

公务邮箱：dudaoqiang@zb.shandong.cn

淄博市市场监督管理局

2023年3月20日

（此件主动公开）

淄博市新材料产业商业秘密保护工作指引

综　述

本工作指引主要适用于新材料产业，其他行业侧重技术研发的企业也可以参考使用。

新材料产业，是淄博市产业转型升级的重要方向，是高技术竞争的关键领域，具有科技含量高、附加值高的特点。因此，新材料企业需要高度重视技术秘密的保护。为了指导新材料企业开展商业秘密保护工作，建立规范的企业商业秘密管理体系，提高企业商业秘密保护水平，切实保护企业创新，防止泄密，依照现有法律、司法解释的规定，在总结实践经验与理论成果的基础上，结合新材料产业特点，制定本工作指引。

本工作指引，由淄博市市场监管局与东岳集团共同起草，桓台县市场监管局给予大力支持和配合。

1 商业秘密的概念

1.1 概念

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。

1.2 构成要件

1.2.1 秘密性

不为所属领域的相关人员普遍知悉，或者不容易获得。

1.2.2 价值性

能够为权利人带来直接的、现实的或者间接的、潜在的经济利益或者竞争优势。

1.2.3 保密性

权利人采取与该信息商业价值、独立获取难易程度等相应的、合理的保护措施，这些保密措施在通常情况下足以防止该信息泄露。

1.3 商业秘密与专利权

1.3.1 权利取得方式不同

专利权是以技术公开为代价，并须通过法定程序的审查而获得；商业秘密则是自主产生或者合法受让获得。

1.3.2 范围与保护客体不同

发明与实用新型专利所保护的是技术方案，外观设计专利保护的是工业应用的新设计；商业秘密保护的是符合商业秘密构成要件的技术信息、经营信息等商业信息，范围相对更为宽泛。

1.3.3 权利基础不同

申请发明和实用新型专利，应当具备新颖性、创造性和实用性，外观设计要富有美感并适于工业应用，且不属于现有设计；商业秘密则要求不为所属领域的相关人员普遍知悉和容易获得。

1.3.4 权利形式不同

专利权在国家机关登记并作公示，具有独占性；而商业秘密是非登记的，且不能公示，商业秘密的权利具有相对性，并不能排斥他人通过其他合法方式而取得并加以实施或利用。

1.3.5 权利状态不同

专利权技术不能因反向工程而合法使用；而商业秘密则会因被公开而丧失秘密性，从而丧失相应权利，而且，他人通过反向工程合法取得产品技术信息的，不认定为侵犯商业秘密。

1.3.6 保护期限不同

专利权具有法定的保护期限，超过法定保护期限相应技术与设计就进入公共领域，任何人均可以使用该项技术与设计；而商业秘密只要采取有效保护措施而不被公开，享有无限期的长久保护。

1.4 综合保护

a）一项技术或者若干项相关联的技术可以将部分内容申请专利，部分内容作为商业秘密加以保护。

b）技术信息在申请专利前或未公开之前，作为商业秘密加以保护。

c）在满足专利申请需要的前提下，将设备参数等核心技术信息，作为商业秘密加以保护。

d）对于技术方案与设计可根据不同情形、不同阶段分别选择专利或商业秘密加以保护。

e）对于能被以反向工程破解的技术方案或设计，不宜采用商业秘密保护方式，可相应以专利权、著作权的权利形式加以保护。

2 管理机构

2.1 领导重视

企业管理层要重视商业秘密保护，尤其是企业主要负责人，以保证企业保护制度贯彻落实。

企业商业秘密保护工作，实行企业主要负责人负责，或者其授权委托人负责，如由技术总工负责技术秘密的管理工作，指导并监督商业秘密管理部门及人员的工作。

2.2 保护管理部门

企业可根据实际经营情况，设置专门的商业秘密保护管理部门，也可以依托法务、技术管理、人事等相关部门，配备专（兼）职人员，承担企业商业秘密管理工作。

2.3 保护管理部门职责

a）研究制定企业商业秘密保护管理制度。

b）研究确定企业商业秘密保护的信息范围、密级划分、保密期限、涉密部门（涉密岗位、涉密人员）、涉密区域以及生产经营各环节保护商业秘密的技术防护措施等事项。

c）组织监督检查业务部门商业秘密保护管理制度落实情况。

d）组织对企业员工进行商业秘密保护教育培训。

e）组织处理企业内部商业秘密泄露事件。

f）开展法律维权，协助有关部门做好商业秘密侵权事件的调查举证等工作。

2.4 部门协作

企业的科技研发、生产经营、人力资源、项目管理等所有涉及商业秘密的业务部门，配备专（兼）职保密员，开展本部门职责范围内商业秘密的保护和管理工作。

3 管理制度

企业应根据经营情况，建立完善商业秘密保护管理制度体系。

a）企业商业秘密保护管理制度。

b）企业涉密文件资料（物资）管理制度。

c）企业涉密设备（计算机）管理制度。

d）企业互联网运行涉密信息管理制度。

e）企业涉密区域（场所）管理制度。

f）企业涉密档案管理制度。

g）企业涉密人员管理制度。

h）企业对外交流及宣传管理制度。

i）企业商业秘密泄露事件处置管理制度。

j）企业研发项目（外部合作）管理制度。

4 定密与分级

4.1 定密

企业应根据经营情况，对涉密的技术信息和经营信息进行核查和评估，确定本企业商业秘密的范围。

由产生该商业秘密的业务部门提出，拟确定的商业秘密及其密级、保密期限、知悉范围等；经商业秘密保护管理部门审核并报领导审批后确定。

4.2 涉密技术信息

a）研发信息：与科学技术有关的设计程序、图纸、模型、样板、测试记录、关键信息资源储备、数据、提议、试验步骤、样品、试验记录、试验方式方法与结论等。

b）生产信息：原料、配方、工艺、流程、样式、技术参数、电子数据、制作方法、技术诀窍等。

c）配置信息：设备仪器的型号、配置参数、特别要求等。

d）软件信息：源代码、应用程序、数据算法等。

e）与业务合作单位协议约定的保密信息

4.3 涉密经营信息

a）公司基础信息：公司组织架构、决议文件、内部通知、规章制度、会议纪要等。

b）决策信息：与经营活动有关的战略规划（计划）、投融资决策、研发策略、商业模式、管理方法、产权交易、股权激励方案、专利规划布局等。

c）经营信息：产购销计划（方案）、产购销协议、招（投）标标书、产购销记录（订单）、运营成本、内部定价文件、产品合格率、库存量、创意管理等。

d）客户信息：客户名单、供应商名单、以及对特定客户的网络电子信息、名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息等。

e）财务信息：财务账簿、财务报表、融资报表、预决算报告、审计报告、股权分配资料等。

f）人力资源信息：员工名册、通讯录、工资表、社保公积金清单等。

g）信息技术信息：应用系统、网络拓扑图、信息安全风险报告、运维日志等。

4.4 分级

企业应对涉密信息进行分级管理，按层级履行审批手续。

涉密信息可分为核心商业秘密、重要商业秘密、普通商业秘密三级，密级可标注为“核心商密”“重要商密”“普通商密”或者“绝密”“机密”“秘密”。

涉密项目负责人应要求研发人员针对研发成果提交技术交底书。项目完成后，项目负责人应召集项目研发人员讨论决定创新成果的发明人及其署名顺序，并提出作为商业秘密保护还是作为专利保护的建议。

4.5 分级参考因素

a）涉密信息的经济价值。

b）企业产生涉密信息投入的成本。

c）涉密信息对企业的重要程度。

d）竞争对手获取涉密信息后产生的价值。

e）涉密信息泄漏后造成的经济损失。

f）涉密信息泄漏后可能承担的法律责任。

g）涉密信息在企业内部可查阅的范围。

4.6 保密期限

企业可根据经营活动实际以及涉密信息的密级等情况，设定保密期限。一般情况下，涉密信息可预见解密期限的，可以年、月、日计；不可预见期限的，可定为“长期”或者“公开前”。

4.7 知悉范围

企业可根据涉密信息的密级以及经营需要，确定知悉范围。

一般情况下，知悉范围应明确限定到具体的业务部门、具体岗位和具

体人员，并按照密级实行分类管理。

4.8 变更

企业根据经营实际，调整涉密信息的密级、保密期限、知悉范围等事项。涉密信息有关事项如需变更的，应履行审核审批程序。

5 解密

5.1 解密

涉密信息出现下列情形时可予以解密：

a）保密期限已满或者信息已公开的（自行解密）。

b）商业秘密已不再具有保护价值。

c）其他特定因素导致涉密信息被公开的。

5.2 解密措施

a）移除涉密区域。

b）消除或变更密级标识。

c）电子文档解密。

d）其他方式。

5.3 销毁

销毁涉及商业秘密的文件（含复制文件）、资料、电子信息、载体和物品，应由保密员列出销毁清单，经商业秘密保护管理部门审批后实施。

5.3.1 销毁过程监督

a）在视频监控范围内销毁。

b）不少于 2 名员工见证下销毁。

c）对销毁过程录像等。

5.3.2 销毁方式

a）文件、资料应粉碎成颗粒状或焚烧处置。

b）电子信息应利用彻底删除软件永久删除，或者物理销毁硬盘、光盘等涉密信息载体。

c）其他合适的方式。

6 涉密信息保护

6.1 文件资料管理

a）应有密级、保护期限等标识，实行登记管理、归档存放，建议以发文形式公布。

b）由部门保密员登记造册，按权限使用，查阅、借阅、续借应履行登记手续。

c）复制（复印、打印、扫描、摘抄等）、跨区域转移、向第三方披露或提供第三人使用前应履行审批和登记手续，复印件或复制件与原件的密级、保密期限相同。

d）新闻发布、论文发表、专利申请等信息发布和公开前，须经商业秘密保护管理部门审核。

6.2 电子信息管理

6.2.1 安全防护

应充分考虑设备、系统的安全性，做好账户、密码的收集、存放和传输的安全工作。

做好病毒防范和病毒库的升级、查杀病毒等工作。定期进行安全检查，发现系统漏洞及时修补。

用户的操作行为应有日志记录，可实时报告登陆、获取信息和异常入侵等行为。

6.2.2 账户、密码管理

对所有涉密账号和密码实行统一登记、备案、发放和变更管理。

各类设备、数据库和应用系统应设账户和密码，不使用默认密码或保

存密码自动登陆。采取适当的账户、密码管理方式，如限制使用简单密码，必要时不定期更改密码，输错密码一定次数锁定账户。

6.2.3 权限管理

应对设备、数据库和各类应用系统及其账户实行权限管理，按岗位职责或特定工作事项，按“最小够用”原则设定权限，合理分配不同层级账户的功能和审批权限。

权限到期、人员转岗、项目或事项变更时应重新授权。

人员离职时应回收相应权限。

6.2.4 数据存储

涉密数据应存储于企业授权的存储设备和应用系统，不应存储于非授权存储设备、网络空间。核心秘密、重要秘密等级的数据应采用加密方式存储。定期对涉密数据进行备份并妥善保存。

6.2.5 保密义务提醒

在账户登陆提示、账户登陆后的主界面设置保密义务提醒；在涉密电子文档首页、页眉、页脚、页面水印等设置保密义务提醒；在涉密音视频开头提示保密义务。

6.3 涉密电子信息流转

a）收发涉密数据应使用唯一出入口，对涉密数据流入流出进行审批。

b）内部局域网应与互联网隔离，涉密数据网络传递应通过内部局域网或加密互联网通道完成。

c）通过邮件发送涉密数据时，应加密和签名，可限定文档打开次数、打开时限和编辑权限等。

d）对外发送涉密数据应经过审批，并采取加密措施，数据发送与密钥发送不宜采用同一通道。

e）与客户、合作单位等涉密数据接收单位或个人签订保密协议。

6.4 涉密载体、涉密物品管理

a）涉密信息存放的硬盘、光盘、磁性介质、U 盘等各类存储设备，应妥善保存、归档登记。

b）涉密载体、物品的存放地点设为涉密重点区域，建议采取物理隔离的方式进行保护。

c）宜对重要原料和部件实行编号替代、分部门管理等管理方式。

d）未经批准，不准许拍摄、测绘或仿造。

e）由部门保密员登记造册，按权限使用，领用应履行登记手续。

f）跨区域转移应履行审批手续，必要时采取防护措施。

g）送外维修前应经商业秘密保护部门审批，并拆卸涉密存储设备。

7 涉密场所管理

7.1 划分涉密区域

企业应按照涉密信息及其载体的密级、性质等，划分为涉密区域、办公区域、外部接待区域三级，列为涉密区域的部门或场所：

a）产品研发设计、实验室、重要生产场所、数据信息存储中心等。

b）信息管理、财务、人力资源等部门。

c）涉密档案室，涉密产品、物品、载体等存放场所。

d）未公开的样品存放地点。

e）模具、专用夹具、重要零部件存放区。

f）重要原材料、重要半成品等涉密物资存放区等。

7.2 涉密区域管理

7.2.1 物理隔离

所有涉密区域应采用门、墙、隔断等物理措施进行防护隔离，形成独立封闭的办公区域。

7.2.2 张贴警示标识

在涉密区域的入口处，应张贴非授权勿入、禁止携带违禁品、禁止拍摄等禁止性警示标识。

7.2.3 设置安防措施

有条件的企业，根据经营需要，可在涉密区域出入口配备安保人员或配置安防设备等，加强对涉密区域的安全防护。

7.2.4 保密与建设同步

涉密区域的新建、改建，要符合保密要求，采取的保密防护措施应当经公司商业秘密管理部门的审核，与工程建设同步计划、同步设计、同步建设、同步验收。

7.3 生产车间保密管理

a）生产工艺流程、图纸等为保密文件，只能由具有查看权限的工作人员查看。对于负责整个生产流程中某一环节的工作人员，只能查看其负责环节的操作手册与图纸，不得查阅权限之外的文件。

b）每个车间应当列明所掌握的所有涉密工艺文件名称，根据实际掌握的文件及时更新该清单，并将该清单与所有涉密工艺文件一起存放于指定的保密文件柜中。

c）每个车间应当及时记录接收、转出、替换、借阅及归还工艺文件的情况。

d）生产工艺流程手册、图纸等一律不得复制、不得带出。有特殊情况的，须报车间领导说明情况，经车间领导签字批准后按照要求进行复制或借出，申请复制或借出的申请表应当建档备查。

e）个人手机严禁带入生产现场，手机一律置于更衣室外透明手机箱中，设专人检查。禁止带入任何照相设备、录像设备、录音设备进入生产现场，因安全生产等要求，需要拍照的，应制定相应细项要求。

f）严禁将生产现场的产品、半成品、原料、配方等一切与产品生产相关的物品带离生产现场。

7.4 涉密生产设备管理

a）涉密生产设备所在区域，应作为涉密区域管理，应有明确保密标识，并禁止外部人员出入。

b）涉密生产设备型号、参数、装配方式、图纸等均不得对外透漏，必要时可以使用内部编码代替。根据实际情况可选择是否与设备供应商签署保密协议，严禁对方透漏任何信息给同行或存在竞争关系的其他企业。

c）涉密生产设备维修、保养、改造时，需要委外处理的，不得透漏与设备自身属性无关的其他信息，必须告知对方时需与对方签订保密合同（协议）。

d）禁止对涉密设备进行拍照，因安全生产等要求，需要拍照的，应制定相应细项要求。不得对涉密设备相关信息进行宣传。

8 员工管理

8.1 入职管理

8.1.1 普通岗位

对非涉密岗位的普通员工，应与其签订劳动合同时，增加商业秘密保密条款，或签订保密协议，明确其应遵守企业商业秘密保护管理规定，及其应履行的与岗位职责、工作内容相适应的保密义务、违约责任等。

8.1.2 涉密岗位员工

对涉密岗位负有保密义务的人员，企业应根据其所在部门、岗位涉密密级、担任的职务以及知晓商业秘密的范围等实际情况，与其签订保密协议，协议中明确其应遵守企业商业秘密保护管理规定，明确应当履行的具体保密义务及违约责任等。

8.1.3 竞业限制

应与高级管理人员、高级技术人员以及其他知悉核心商密、重要商密的人员，签订竞业限制协议，明确竞业限制的范围、地域、期限、违约责

任等；在解除或终止劳动合同后的竞业限制期限内，约定给予的经济补偿及违约金额等。

8.1.4 预防员工侵权

对入职员工曾在与本企业有（或潜在有）竞争关系的企业工作经历的，应当在劳动合同中增加承诺不侵犯原企业商业秘密的条款，或签订不侵犯原企业商业秘密的协议，明确规定入职员工在本企业工作期间不得使用、公开、泄露原单位的商业秘密。

8.2 在职管理

8.2.1 保密教育培训

企业应制定年度员工保密教育培训计划，组织新入职员工、重点岗位、重要涉密人员以及全体员工参加有针对性的保密教育培训。

员工教育培训有关材料应进行登记存档。

8.2.2 履职监督检查

企业商业秘密保护管理部门应会同业务部门，定期对在职员工履职过程中，执行企业商业秘密保护管理制度情况进行监督、检查。

对员工履职情况监督检查的记录应进行登记存档。

8.3 调岗管理

涉密岗位员工调整岗位时，商业秘密保护管理部门应安排专人与其谈话，告知其应承担的保密义务和相应的法律责任，监督其办理涉密信息资料和涉密物品的交接手续。

涉密员工调岗及交接情况应进行登记存档。

8.4 脱密期管理

对涉密员工调岗或离职实行脱密期管理。企业应根据员工岗位涉密的密级确定脱密期限，同时采取相应措施，确保涉密员工在脱密期内继续按

照规定履行保密义务，不得以任何方式泄露商业秘密。

8.5 离职管理

8.5.1 离职谈话

与离职员工谈话，告知应承担的保密义务，以及违反规定要承担的法律责任。

8.5.2 离职交接

制作离职员工工作交接清单，列出离职员工应移交的所有涉密文件资料、电脑等硬件设备、账号、密码、数据及其载体等，安排专人与其办理交接手续，逐项核对回收其保管的所有涉密物品。

8.5.3 回收账号权限

回收并注销离职员工使用的域名、应用系统、网络系统、门禁系统账号或访问权限等。

8.5.4 离职涉密检查

检查离职员工所负责的涉密信息，在一定期限内的查阅、使用情况有无异常，电子数据信息是否完整，有无非工作时间登录、频繁登录、更改账户、批量下载、删除修改、访问外部邮箱等违规和异常操作痕迹等。

如发现离职员工涉嫌侵害企业商业秘密的，应及时收集并固定证据，按照商业秘密泄露事件管理规定处置。

8.5.5 通知客户

及时通知与离职员工有关的供应商、客户、合作单位，告知工作交接情况。

8.5.6 离职跟踪

应定期掌握涉密离职员工在竞业限制期限内的任职去向，如发现离职

员工存在竞业限制情形的，视情启动竞业限制，维护企业权益。

9 商务活动管理

9.1 基本要求

a）企业开展商务谈判、技术评审、成果鉴定、合作开发、技术转让、外部审计、清产核资等商务活动时，涉及商业秘密的，应与相关方签订保密合同（协议），或在商务合同（协议）中规定涉密信息保密要求，约定具体的保密内容、范围、保密期限、保密责任义务及违约责任等。

b）双方签订的保密合同（协议）应进行登记存档。

c）注意留存双方往来的与涉密信息有关的原始信息资料（包括网络媒介传输的电子信息），并应在交付资料上注明保密标识及权利归属，交付资料列明清单由对方人员签字确认。

9.2 技术合作

a）技术转让、委托研发、共同研发等技术合作，应在合同中明确技术成果的使用权、转让权以及收益的分配方式。如不作明确约定，双方都有使用和转让的权利。

b）技术合同中明确保密义务或者单独签订保密合同，明确要求对方与其相关员工签订保密合同。

c）技术研发使用企业商业秘密的，要在合同中明确保密内容、范围、保密期限，经批准后提供；在提供的资料上有保密标志；传递需通过加密途径；对商业秘密使用情况进行监督管理。

9.3 外聘人员管理

a）企业聘用或委托外聘的专家、顾问、律师等可能接触企业涉密信息的，应与其签订保密合同（协议）或签订保密承诺书。

b）应要求使用企业提供的保密计算机，并对信息采取加密等措施。

c）注意留存双方往来的与涉密信息有关的原始信息资料（包括网络媒介传输的电子信息）。

9.4 外来人员管理

a）需要外部人员参与的项目，可根据项目重要程度选择与对方项目参与人员分别签署保密合同（协议），并进行相关保密培训。

b）企业需要向行政机关、具有行政管理职能的事业单位等外部单位提供的资料，涉及商业秘密的，应明确告知涉密信息事项、保密义务等。

c）外来参访人员进入公司需要进行登记，并由来访人员签字。参访人员应当按照指定的路线参观，并由企业人员全程陪同。

d）对于需要参观车间、实验室、控制室等涉密区域的参访人员，由接待部门报商业秘密管理部门审批，并签署保密承诺书。参访人员不得携带任何拍照、录音录像、存储设备、磁性物质等。在参观前，应进行安全检查。

9.5 涉密会议接待

企业组织召开会议、承办的其他商务活动或接待来访人员涉及商业秘密的，应采取以下保密措施。

a）选择有保密条件的场所。

b）限定参加人员的范围，指定参与涉密事项的人员。

c）告知参加人员保密要求，必要时签订保密承诺书。

d）设定参加人员活动区域。

e）限定参加人员使用拍照、摄像、录音、信息存储等设备。

f）对相关会议资料（包括宣传片、文件资料等）尽量进行脱密处理。

g）对涉密文件进行编号管理，休会或活动结束及时收回清点、登记涉密文件资料等。

10 泄密事件处置

10.1 应急处置

a）应制定商业秘密泄密紧急处理预案，建立泄密事件紧急应对流程。

b）如发现企业涉密信息泄露线索时，应迅速处置，采取补救措施，防止涉密信息进一步扩散或损失扩大。

c）启动对商业秘密泄露事件的调查，查明原因、涉事人员和责任人。

d）搜集并固定有关商业秘密泄露的证据。对商业秘密泄露、侵权所造成的损失进行评估鉴定。

10.2 收集固定证据

a）证明企业是涉案商业秘密的权利人。

b）涉案商业秘密的具体内容和载体。

c）涉案商业秘密不为相关公众普遍获知，不为相关公众容易获得。

d）企业对涉案商业秘密采取的保密措施。

e）泄密人员、侵权人的身份信息。

f）泄密人员、侵权人接触涉案商业秘密的证据，以不正当手段获取、披露、使用涉案商业秘密等侵权行为的证据。

g）企业被侵权造成的损失或侵权人的获利。

h）企业主张法定赔偿的参考因素及其证据

10.3 维权途径

a）向市场监督管理部门投诉举报。

b）向公安机关报案。

c）申请劳动仲裁或商事仲裁。

e）向人民法院提起民事诉讼。

f）向人民检察院提起商业秘密诉讼活动法律监督等。