淄博市市场监督管理局

关于印发《淄博市小微企业商业秘密保护工作指引》的通知

各区县市场监管局：

探索建立分行业领域的企业商业秘密保护规则体系，研究制定一批符合行业特点和产业发展需求的商业秘密保护规则指引，是省、市加强商业秘密保护三年行动计划确定的重点任务.近期，市局已经编写新材料产业、医药产业的商业秘密保护工作指引。为了增加工作指引的覆盖面，全面提高企业商业秘密保护水平，市局编写了《淄博市小微企业商业秘密保护工作指引》，现印发给你们，作为开展企业商业秘密保护行政指导的工作资料，供我市小微企业参考使用。

各区县市场监管局要认真收集企业在商业秘密保护工作中，好的做法、经验、意见和建议，请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 5 月 16 日

（此件主动公开）

淄博市中小企业商业秘密保护工作指引

目 录

本工作指引主要适用于经营规模相对较小、需要保护的商业秘密略少的小微企业。

小微企业的经营规模虽小，但也普遍存在需要保护的商业秘密。根据商业秘密保护的合理性、适当性原则，小微企业可以根据经营情况、商业秘密重要程度等因素，采取适当的保密措施。本指引提供的常用保密措施中，制定保密制度和签订保密协议是基本的保密措施，建议小微企业在此基础上根据自身情况选择使用其他保密措施，鼓励企业尽可能多的选择。有条件的企业，建议参照我们编写的其他行业性商业秘密保护工作指引，建立更为完善的商业秘密保护体系。

1 商业秘密

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。（《中华人民共和国反不正当竞争法》第九条）

构成商业秘密的第一要件，是权利人主动保护，采取与商业秘密的商业价值、独立获取难易程度等相应的、合理的保护措施。

企业要结合需要保护的技术信息或者经营信息的特点，综合运用商业秘密、专利、版权等进行保护，比如将商业秘密隐藏在专利技术之下。

2 定密

确定需要保护的商业秘密（密点），是商业秘密保护的基础性工作。

可以确定为商业秘密的信息，主要有技术信息和经营信息。

2.1 技术信息

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。

2.2 经营信息

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。

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，是在交易过程中形成的特定交易需求、价格范围、交易习惯等，区别于相关公知信息的特殊客户信息，要符合商业秘密“不为公众所知悉”的构成要件。

2.3 定密要求

a）企业应定期或者根据经营需要及时进行梳理，并确定密点。

b）密点的确定，要尽可能做到精准，达到最小化原则。

c）形成密点（特别是技术信息）的资料要留存：

一是企业自主研发获取的商业秘密。可通过研发立项、记录文件、试验数据、技术成果验收备案文件等证明商业秘密的形成及归属，有条件的企业，可以采用时间戳等技术手段保存证据资料。

二是继受取得，通过交易方式受让或取得使用授权。可通过交易转让合同或授权使用许可协议等材料证明商业秘密的归属或使用权利。

d）商业秘密具有无形性，商业秘密的内容必须通过有形的载体予以呈现。根据密点，确定商业秘密的内容，也就是确定商业秘密的保护范围，明确具体的载体形式。

3 保密措施

商业秘密与专利等知识产权最大的不同，在于需要权利人主动保护。没有采取保密措施的，构不成商业秘密，就无法获得行政、司法上的保护。

3.1 原则性要求

a）合理性。企业可根据商业秘密及其载体的性质、商业价值，采取适当的、合理的保密措施。在正常情况下，要能够达到防止商业秘密泄露的目的。

b）可识别性。采取的保密措施，要能体现出企业保护自身商业秘密的意愿，比如采取了限制性措施，禁止他人访问涉密车间。

c）证据留存。采取的任何保密工作，要做到“留痕”，做到一旦出现泄密事件，能够追查泄密人和泄密途径，能够提供出有效的证据。

d）兼顾工作便利性。侧重保护的同时，采取的保密措施还要兼顾工作的便利性，做好二者的平衡。

e）防止侵犯他人商业秘密。坚守诚信，不做侵犯他人商业秘密的行为。录用新员工时，做好背景调查，告知有保密义务的员工不使用其在以前工作的单位掌握的涉密信息，防止被告侵权。

3.2 常用保密措施

下列保密措施，企业可以根据情况自行选择使用，建议企业采取尽可能多的保密措施。其中，制定保密制度和签订保密协议是基本，建议企业必选；员工保密培训，涉密岗位人员的重点培训，是基本要求；对涉密信息进行分级管理，合理的划分权限，能够减少保密工作对生产经营的影响，建议企业优先选用；采取加密、隔离等手段，限制他人访问、参观和接触涉密计算机、设备和车间等，是比较实用的保密措施。

a）签订保密协议或者在合同中约定保密义务。

b）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。

c）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。

d）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。

e）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。

f）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。

4 保密制度

企业可参照附录的参考文本，结合自身经营情况，制定商业秘密保护管理制度。

保密制度制定后，要让员工知悉，可以由企业正式行文发布，编制员工手册，组织员工学习，将学习签到、拍照录像等培训资料、其他方式让员工知悉的记录等，做好存档。

5 保密协议

5.1 员工保密协议

企业应根据岗位涉密情况，在与员工签订相应的保密协议，明确应遵守的企业商业秘密保护管理规定，以及其应履行的保密义务及违约责任等。违约责任部分，可以明确约定一个具体的金额，一方面起到对员工的警醒，另一方面可以用于企业事后维权对于损失的举证。

保密协议要对商业秘密的类型、载体作出明确约定，保密费并非保密协议的当然条款。

5.2 竞业限制协议

对于高级管理人员、高级技术人员等重要岗位员工，建议签订竞业限制协议，建议在职期间就签订，不要只是在员工离职时签订。

5.3 商务活动保密协议

企业在对外开展经营活动时，涉及商业秘密的，应与相关方签订保密协议，或在商务合同（协议）中规定涉密信息保密要求。

6 分级

涉密信息可分为两级，核心商业秘密和普通商业秘密，密级可标注为“核心商密”和“普通商密”，或者“绝密”和“秘密”。

企业可根据经营需要，确定知悉范围，坚持“无需要不接触”原则，只让因工作需要必须知悉的人员接触。

7 权限管理

7.1 合理设定权限

应对涉密文件、设备、数据库和各类应用系统及其账户实行权限管理，根据岗位职责或特定工作事项，按“最小够用”原则设定权限，合理分配不同层级的权限。

7.2 离职收回

人员离职时，应回收相应权限。

人员调整岗位时，应相应的调整权限设置。

7.3 审批制度

未经批准，不得复制（复印、打印、扫描、摘抄等）涉密资料，不得擅自对外发布、发表，不得擅自传给他人。审批流程，应当存档。

对外发送涉密信息，应对知悉范围和权限进行控制。

8 保密标识

对涉密信息及其载体实行标识管理。

8.1 标识内容

标识由名称或编号、密级、保密期限以及权属单位组成，可以根据需要作适当简化。

8.2 加贴标识

在涉密信息的所有载体上的醒目位置，加贴保密标识。

涉密信息设备或涉密存储介质应当在醒目位置粘贴不易损毁或篡改的专用标识。

9 警示标识

9.1 保密提醒

涉密计算机等设备、数据库及应用系统等账户登录、系统操作界面等各类应用场景中，应进行保密义务提醒。

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；涉密音（视）频开头应进行保密义务提醒。

9.2 禁止性警示

非涉密办公设备粘贴“严禁处理涉密信息”等保密警示标签。

在涉密场所的入口处，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。

10 信息加密

对涉密信息采取加密、加锁、反编译等预防措施。

对于涉密信息采用密码或者代码等，如使用代码替换某些重要的材料真实名称。

涉密数据存放在专用设备，并做加密处理。

涉密电子信息网络流转应使用内部局域网或互联网加密通道方式进行传输；通过电子邮箱发送涉密电子信息时，应采用内容加密、设备绑定、限定打开次数、打开时限、编辑权限等保密措施。

11 涉密载体管理

涉密文件、涉密物品、存放涉密信息的各类存储设备，由专人保存管理，存放在有安全防护措施的地方。

对重要原料和部件实行编号替代，或者采取分部门管理方式。

12 涉密场所管理

对于涉密的机器、厂房、车间、计算机房、档案室等场所限制来访者，采取基本的物理隔离措施，如门禁、监控、权限控制等，在入口处和其他醒目位置张贴禁止性警示标志。

有条件的企业，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。

13 员工管理

保护商业秘密，重在人的管理和防控。

13.1 签订协议

签订保密协议和竞业限制协议，是重要的管理手段。

13.2 保密培训和警示教育

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，进行警示性教育，提高员工保守秘密的意识。

13.3 离职管理

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。

与离职员工谈话，告知应承担的保密义务，要求其继续承担保密义务。

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。

14 常见侵犯商业秘密行为

a）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。

b）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。

c）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。

d）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。

e）第三人明知或应知上述四项侵权行为，仍获取或披露或使用或允许他人使用商业秘密。

15 泄密事件处置

发生泄密事件后，应尽快核实泄密内容，调查泄密原因，查找责任人，并要及时收集固定相关证据。

经验不足的企业，可以及时聘请律师等专业人员，可以与市场监管部门、公安机关联系，在其指导下收集证据。

15.1 权属证据

能证明商业秘密权属的证据，包括技术秘密和经营秘密的载体，可以是纸质文件，如图纸形式，也可以用光盘刻录。

15.2 秘密性证据

证明不为相关公众所知悉或容易获得。如不为公众所知悉的鉴定意见等证据。

15.3 保密措施证据

证明采取了相应的保密措施，包括保密制度、保密协议、保密培训、保密警示、提出保密要求等。

15.4 接触商业秘密证据

主要包括企业与员工之间的劳动合同、保密协议、离职文件，围绕涉案侵权人曾接触过企业的商业秘密收集并固定证据。

15.5 侵权行为证据

侵权行为证据多种多样，如涉案侵权人利用商业秘密申请专利、制造产品，与企业的客户进行交易等。

15.6 被侵权造成的损失

权利人受到的实际损失、侵权人因侵权所获得的利益、商业秘密的许可价值、侵权人恶意重复侵权、合理开支等。

如造成损失或者违法获益超过 30 万元，或者直接导致权利人因重大经营困难而破产、倒闭的，应由公安机关立案追究刑事责任。

16 举证责任转移

权利人有证据证明涉案侵权人所使用的信息，与权利人的商业秘密实质上相同；同时能证明涉案侵权人有获取其商业秘密的条件。而涉案侵权人不能提供或者拒不提供证据，证明其不存在侵犯商业秘密行为的，可以根据有关证据，认定涉案侵权人的侵权行为成立。

17 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。