

DB3202

无 锡 市 地 方 标 准

DB3202/T 1058—2023

商业秘密保护服务规范

2023 – 12 – 31 发布

2024 – 01 – 08 实施

无锡市市场监督管理局

发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 1

5 企业自主保护 2

6 依法保护 3

7 协同保护 4

8 服务评价与改进 5

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由无锡市市场监督管理局提出并归口。

本文件起草单位：无锡市市场监督管理局、江阴市市场监督管理局、滨湖区市场监督管理局、江南大学、无锡市检验检测认证研究院。

本文件主要起草人：须蒙凯、耿敬鹏、庞博、潘文伟、张立、徐杰、孙元宏、彭晶瑶、吴国科、顾成博、姚志娟、郑菲、陈强。

商业秘密保护服务规范

1 范围

本文件规定了商业秘密保护服务的术语和定义、基本原则、企业自主保护、依法保护、协同保护和评价与改进的要求。

本文件适用于企业集聚的园区管理机构、行业协会、商会等行业组织、第三方社会服务机构商业秘密保护服务工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 19001 质量管理体系 要求
- GB/T 22080 信息技术 安全技术 信息安全管理要求
- GB/T 29490 企业知识产权合规管理体系 要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

商业秘密 trade secrets

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。

3.2

技术信息 technical information

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。

3.3

经营信息 commercial information

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。

4 基本原则

4.1 自主保护

指导企业增强商业秘密保护主体意识，引导企业采取管理、技术、经济等手段，实施商业秘密自主保护。指导企业提高商业秘密保护能力，建立企业商业秘密保护机制和制度，识别和确定商业秘密的泄密风险，加强保密事项的管理，并采取相应的保护和应急措施，预防或避免商业秘密泄密或被侵犯的行为发生。

4.2 依法保护

指导企业在商业秘密受到侵犯时，要理性表达利益诉求，依据相关法律法规的规定，向行政部门、司法部门等寻求保护，维护合法权益。

4.3 协同保护

提供宣传培训、技术咨询、法律援助等服务，提高商业秘密保护能力。

5 企业自主保护

5.1 管理组织

指导企业设立商业秘密管理组织，为商业秘密保护工作创造条件，确保商业秘密保护工作有效运作。商业秘密管理组织包括但不限于：

- a) 管理决策机构；
- b) 办事执行机构；
- c) 监督议事机构。

5.2 商业秘密管理

指导企业按下列要求管理商业秘密：

- a) 建立商业秘密保护制度；
- b) 界定商业秘密和相关信息载体的保护范围；
- c) 确定商业秘密的保密等级和保密期限；
- d) 设置物理隔离区域，配置安全防护和监控设施，设置明显的警示隔离标志；
- e) 管控知悉范围，根据实际生产经营需要将商业秘密控制在最小知悉范围内；
- f) 规范商业秘密流转流程与要求，并保留流转记录；
- g) 与相关员工签订保密协议、竞业限制协议等；
- h) 规范外来访客要求，划分公共开放区域，记录访客信息；
- i) 建立涉密审查前置程序；
- j) 组织开展新员工保密、业务保密、专项保密、脱密保密等培训；
- k) 巡视检查商业秘密保护制度和保密措施的贯彻落实情况、商业秘密防护设施和监控设施的运行情况，详细记录检查情况并形成书面报告。

5.3 风险防范

指导企业参照GB/T 19001、GB/T 22080、GB/T 29490的要求建立风险防范体系，建立包括但不限于下列内容的风险防范机制：

- a) 风险监测机制；
- b) 风险评估机制；
- c) 风险预警机制；

d) 风险应对机制。

5.4 应急处置

指导企业开展应急处置，包括但不限于下列内容：

- a) 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) 培训和引导员工对商业秘密可能泄露的异常状态保持警觉，发现可能泄密迹象及时报告上级；
- c) 出现商业秘密泄露的征兆或者迹象时，企业应：
 - 1) 迅速进行处置，防止信息扩散；
 - 2) 启动对商业秘密泄露的核查、确认和评估，查明原因、责任人；
 - 3) 采取措施，将危害和损失控制在最小限度内等。

5.5 持续改进

指导企业根据前述商业秘密基本原则以及检查、分析的结果，持续改进商业秘密保护体系，制定和落实改进方案与措施，跟踪改进状况，确保改进到位。

6 依法保护

6.1 维权途径

指导企业发现商业秘密泄密后，依法采取以下维权途径：

- a) 举报控告：
 - 1) 向市场监管部门投诉举报；
 - 2) 符合刑事案件立案标准的可向犯罪地的公安机关控告。
- b) 诉讼维权：
 - 1) 申请劳动仲裁或商事仲裁；
 - 2) 向人民法院提起民事诉讼。
- c) 涉及国家秘密的，应立即向当地公安机关、国家安全机关、保密行政管理部门报告，并采取补救措施。

6.2 证据搜集与固定

6.2.1 指导企业发现商业秘密涉嫌被侵权时，搜集并整理下列证据性材料：

- a) 企业是该商业秘密的权利人的证据：
 - 1) 商业秘密权利人主体信息、侵权人主体信息；
 - 2) 泄密信息的具体内容、载体；
 - 3) 商业秘密自主研发/开发的相关证明材料或有关转让授权材料；
 - 4) 泄密信息为一般公众不知悉或者无法轻易获得的证明；
 - 5) 具有现实或者潜在的商业价值证明；
 - 6) 已采取的保密措施。
- b) 合理表明该商业秘密被侵犯的初步证据：
 - 1) 泄密人员能够接触秘密信息且被侵权信息与该秘密信息实质相似的初步证据；
 - 2) 泄密人员相关信息：包括签订劳动合同/保密协议、参与的保密培训、具体工作职责等信息；
 - 3) 可能的泄密途径。

c) 该商业秘密被侵犯的损害事实:

- 1) 侵权行为具体表现(如非法获取、非法披露、非法使用等);
- 2) 被侵权所受的损失或侵权行为所获得的收益;
- 3) 主张法定赔偿的参考因素及其证据。

6.2.2 指导企业向商业秘密保护服务机构寻求帮助。

6.2.3 指导企业向专业机构申请涉密信息的非公知性、同一性和损失数额的鉴定。

6.2.4 指导企业向公证处等机构申请电子数据类证据公证或证据固化。

7 协同保护

7.1 基本要求

7.1.1 园区管理机构、行业协会、商会等行业组织以及第三方服务机构等提供商业秘密保护工作支持,提高企业商业秘密保护工作能力。服务资源包括但不限于以下方面:

- a) 商业秘密保护宣传培训;
- b) 商业秘密管理建设等;
- c) 涉密信息的信息管理系统的开发、部署和维护;
- d) 商业秘密侵权风险监测与预警;
- e) 商业秘密信息鉴定或评估;
- f) 商业秘密维权协助。

7.1.2 园区管理机构、行业协会、商会等行业组织以及第三方服务机构等可根据自身力量和企业需求。聚集、整合商业秘密保护的服务资源,提供商业秘密保护宣传、咨询、指导、风险监测、维权等服务,为行政部门、司法部门等开展商业秘密保护服务工作提供协助。

7.2 服务内容

7.2.1 培训服务

7.2.1.1 采取学术论坛、专题讲座、案例研讨、法规解释、政策解读、展板陈列、知识竞赛等线上或线下方式,开展商业秘密保护宣传。宣传渠道包括但不限于:

- a) 新闻媒体;
- b) 网络短视频;
- c) 网络直播;
- d) 微博;
- e) 微信公众号;
- f) 实体区域:
 - 1) 产业园区;
 - 2) 经济开发区;
 - 3) 保护示范点;
 - 4) 保护联系点。

7.2.1.2 制定宣传培训方案,定期组织企业开展商业秘密保护宣传培训。提供适合企业不同层次人员的商业秘密保护专题培训:

- a) 对企业股东、高级管理人员开展商业秘密保护重要性、必要性和战略性的培训;
- b) 对企业从事商业秘密保护工作的专(兼)职人员、重点岗位人员开展商业秘密保护实务及案例培训;

- c) 对企业员工开展商业秘密保护知识培训和警示教育;
- d) 将维权成功的案例向企业广泛宣传等。

7.2.2 指导服务

7.2.2.1 政府组建指导网络,联系相关行政及司法部门,为企业开展商业秘密保护体系建设提供指导与服务。

7.2.2.2 通过走访调研,了解企业商业秘密保护需求,有针对性地开展商业秘密保护指导工作。

7.2.2.3 接待和解答企业商业秘密保护咨询,提供商业秘密保护相关资料查询服务。开放接待日,接受商业秘密保护方面的咨询。

7.2.2.4 对企业商业秘密保护工作进行风险评估,指导企业发现商业秘密保护工作的漏洞。

7.2.2.5 引导企业建立和完善商业秘密保护工作体系,包括:

- a) 界定商业秘密保护范围;
- b) 建立和完善商业秘密保密制度;
- c) 建立和完善商业秘密分级分类管理制度;
- d) 建立和完善商业秘密使用管理制度;
- e) 建立和完善商业秘密保护的应急反应机制等。

7.2.2.6 具备条件的园区管理机构、行业协会、商会等行业组织以及第三方服务机构等可依相应服务资质提供下列专业服务:

- a) 开发、部署和维护涉密文件、数据的信息管理系统;
- b) 提供技术信息的非公知性、同一性和损失数额的鉴定评估;
- c) 提供科技查新委托服务;
- d) 协助被侵权企业搜集证据和维权;
- e) 其他专业服务。

7.2.2.7 指导企业建立健全商业秘密保护制度、商业秘密泄密工作预案等。

7.2.2.8 指导企业开展商业秘密保护风险与漏洞排查,并进行风险评估和风险提示。

7.2.2.9 指导企业收集侵犯商业秘密的证据。

7.2.2.10 指导企业建立商业秘密保护联盟,培育商业秘密保护示范典型。

7.2.2.11 具备条件的园区管理机构、行业协会、商会等行业组织以及第三方服务机构等可建立商业秘密保护服务网络。

7.2.3 风险监测

7.2.3.1 具备条件的园区管理机构、行业协会、商会等行业组织以及第三方服务机构等可对辖区/行业内商业秘密侵权突发事件、隐患、可能出现的紧急情况开展风险监测。

7.2.3.2 根据发生的商业秘密侵权案例、服务过程中发现的商业秘密泄露隐患,向企业发布商业秘密风险警示。

7.2.4 协助维权

7.2.4.1 当企业反映商业秘密被侵犯并寻求帮助时,提供协助搜集、整理维权材料等服务。

7.2.4.2 根据被侵权企业意愿,协助执法部门开展泄密核查、现场检查等行动,并配合做好调解服务。帮助企业制定维权方案,联系和协调有关部门。

8 服务评价与改进

8.1 服务评价

8.1.1 服务评价内容包括但不限于企业自主保护、依法保护、协同保护的服务完成情况、服务规范情况、满意度测评情况、其他相关方反馈情况等。

8.1.2 服务评价可采用自我评价、服务对象评价和第三方评价等方式。

8.2 服务改进

8.2.1 应根据服务评价结果发现服务过程中存在的问题，并分析原因。

8.2.2 应根据存在的问题和原因确定服务改进目标和内容，制定服务改进措施。

8.2.3 应落实服务改进措施，持续提升服务质量。
