

DB3202

无 锡 市 地 方 标 准

DB3202/T 1059—2023

企业商业秘密保护体系建设规范

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 2

5 管理组织 2

6 商业秘密的管理 3

7 风险防范 7

8 评价与持续改进 9

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、工装自控工程（无锡）有限公司、贝卡尔特（中国）技术研发有限公司。

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、奚烨锋、王剑伟。

企业商业秘密保护体系建设规范

1 范围

本文件规定了无锡市企业商业秘密保护体系建设的基本原则、管理组织、商业秘密保护、风险防范的要求。

本文件适用于无锡市企业开展商业秘密保护体系建设工作。

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 信息安全管理体系要求

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 secret

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

涉密物品 secret-related item

含有商业秘密信息的设备和产品。

3.3

涉密载体 secret-related carrier

以文字、数据、符号、图形、图像、视频和音频等方式记录商业秘密信息的介质。

3.4

涉密计算机 secret-related computer

处理或存储商业秘密信息的台式机、便携机、一体机、平板等各类计算机。

3.5

涉密区域 secret-related area

含有商业秘密信息、人员进入后可能接触到商业秘密的物理区域。

4 基本原则

4.1 主动保护原则

企业商业秘密保护体系建设应遵循下列主动性特点：

- a) 企业能够主动地将特定技术信息、经营信息等商业信息确定为商业秘密；
- b) 企业能够主动地表明具有保护前述商业信息的主观意愿；
- c) 企业能够主动地对前述商业信息采取客观上能够被识别的相应保密措施；
- d) 企业能够主动地对商业秘密侵权风险进行监测、评估、预警和应对。

4.2 有效保护原则

企业商业秘密保护体系建设应注重商业秘密保护措施的有效性。在研究制定保密制度和采取保密措施时，应根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度等因素进行综合考虑。

4.3 规范保护原则

企业商业秘密保护既要保护商业秘密权利人的利益，也要保护企业员工的合法权益。企业商业秘密保护的管理工作应实现制度化和规范化，不仅使商业秘密保护成为企业经营管理的重要组成部分，也要使商业秘密保护的方式方法更为规范化和科学化。

5 管理组织

5.1 管理决策机构

5.1.1 设立商业秘密管理决策机构，统一领导商业秘密保护制度和保护措施建设，贯彻落实商业秘密保护要求，研究决定商业秘密保护工作的相关事项。

5.1.2 商业秘密管理决策机构的负责人应由企业的法人代表或者主管人员担任，其成员应由保密办公室负责人和各业务部门负责人（如：技术、生产、销售、财务、人事、法务、信息技术等部门的负责人）组成。

5.2 办事执行机构

5.2.1 在商业秘密管理决策机构之下设立保密办公室作为日常办事执行机构，并配备专职保密人员负责企业日常保密工作的开展和保密事务的处理。

5.2.2 企业保密办公室的工作职责具体包括但不限于下列内容：

- a) 负责企业商业秘密保护的日常管理工作；
- b) 拟定商业秘密保护制度和保护措施，报请企业商业秘密管理决策机构核准执行；
- c) 组织和开展商业秘密保护培训，提升企业员工的保密意识和保密技能；
- d) 协同企业各业务部门落实商业秘密保护制度和执行保密措施；
- e) 定期巡视检查商业秘密保护情况，并对相关问题提出解决方案。

5.3 监督议事机构

5.3.1 设立由董事、监事、高级管理人员等组成的商业秘密监督议事机构，统一负责对企业商业秘密保护体系建设工作和商业秘密保护日常工作进行监督，并参与相关重要事项的研讨。

5.3.2 企业商业秘密监督议事机构应按照商业秘密保护制度规定履行监督职责，其监督职责具体包括但不限于以下内容：

- a) 监督企业管理决策机构和办事执行机构的工作人员履职情况，对违反保密制度规定的工作人员提出罢免建议；
- b) 监督企业各业务部门的商业秘密保护制度和保护措施落实情况，对贯彻执行效果不佳的业务部门提请管理决策机构予以纠正；
- c) 监督企业商业秘密保护政策是否存在侵犯企业员工利益的情况，对于损害企业员工利益的制度或措施提请管理决策机构予以修改和完善。

5.4 组织运作保障

5.4.1 企业商业秘密管理决策机构、办事执行机构、监督议事机构应紧密合作，创造商业秘密保护工作条件、提升商业秘密保护工作效率、保障商业秘密保护工作经费、确保商业秘密保护体系有效运作。

5.4.2 企业相关业务部门应在各自业务范围内配合企业保密办公室完成商业秘密保护的日常工作，落实企业商业秘密保护制度，完善商业秘密保护措施，开展商业秘密保护培训，防范商业秘密保护风险。

5.5 保密绩效评价

5.5.1 企业应建立科学的商业秘密保护绩效评价标准。

5.5.2 商业秘密保护绩效评价标准的设置应综合考虑下列因素：

- a) 企业业务部门落实商业秘密保护制度的主动性；
- b) 采取商业秘密保护措施的有效性；
- c) 部门人员参加商业秘密保护培训的比例；
- d) 部门人员违反商业秘密保护制度规定的次数和严重性；
- e) 发生其他商业秘密保护安全风险的次数和严重性。

6 商业秘密的管理

6.1 建立规章制度

企业保密办公室应制定企业商业秘密保护制度、企业员工商业秘密保护手册等商业秘密保护政策性文件，营造保密文化氛围。

6.2 保护范围界定

6.2.1 企业保密办公室应协同相关业务部门共同确定本企业的商业秘密及相应载体的保护范围，并根据生产经营的实际情况定期审核和动态调整本企业商业秘密及相应载体的保护范围。

6.2.2 企业应将符合商业秘密构成要件的下列商业信息确定为本企业的商业秘密，其保护范围也应包括下列相关商业信息的载体：

- a) 技术信息：即与技术有关的结构、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；
- b) 经营信息：即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；
- c) 其他符合商业秘密构成要件的商业信息。

6.3 密级期限设定

6.3.1 企业保密办公室应协同相关业务部门共同确定本企业各项商业秘密的保密等级和保密期限，并根据生产经营的实际情况定期审核和动态调整本企业商业秘密的保密等级和保密期限。

6.3.2 企业宜根据信息泄露对本企业经济利益和竞争优势的损害程度，将商业秘密的密级确定为核心秘密和普通秘密两级，或者确定为秘密、机密、绝密三级。

6.4 物理隔离防护

6.4.1 企业保密办公室应设置专门的商业秘密保密室，用于存放和保管商业秘密的存储载体或者含有商业秘密的物理载体等涉密载体。商业秘密保密室应与企业办公区域相互隔离，配置安全防护和监控设施，设置明显的警示隔离标志，并由专职保密工作人员负责日常管理。

6.4.2 企业涉及商业秘密研发和使用的工作区域（如：实验室、厂房、车间等生产经营场所）应与其他工作区域相互隔离，配置安全防护和监控设施，设置明显的警示隔离标志，不同区域之间的人员流动需要符合保密隔离的制度要求。

6.4.3 企业内部网络系统应与外部互联网系统相互隔离，配置网络安全防护和监控设施，企业的日常工作安排、任务下达、资料传递、信息交流等活动应在内部网络系统中进行。企业保密办公室应当协同网络管理业务部门负责企业内部网络系统的安全管理，并在网络后台持续监测企业员工搜索、浏览、下载、传输商业秘密的行为是否存在异常情况。

6.4.4 企业为员工配置的用于工作的计算机、存储设备等电子设备应与其他外部传输设备相互隔离，并配置电子设备的安全防护和监控设施。企业员工的日常工作应在企业配置的电子设备中完成，未经许可不得连接外部电子设备和擅自传输企业商业秘密。

6.5 知悉范围管控

6.5.1 企业保密办公室应协同相关业务部门共同确定不同部门和不同级别的涉密人员对不同等级商业秘密的知悉范围，并以明示方式在企业涉密人员范围内予以公示，涉密人员应签字确认其知悉情况并承诺遵守保密规定。

6.5.2 企业保密办公室应根据实际生产经营需要将商业秘密控制在最小知悉范围之内，涉密人员原则上不得跨级别和跨部门接触和知悉保密权限以外的商业秘密。如果涉密人员因工作需要必须知悉保密权限以外的商业秘密，应报请业务主管部门和保密办公室批准并备案。报请事项应当一事一议，并在工作任务结束后终止相关人员的知悉权限。

6.5.3 企业保密办公室在划分商业秘密知悉范围时宜考虑下列因素：

- a) 企业员工所在业务部门；
- b) 企业员工的工作职务、职责、权限；
- c) 企业员工的本职工作或者临时任务与相关商业秘密的关联程度；
- d) 其他需要考虑的因素。

6.5.4 企业保密办公室宜通过设置下列措施分级管控涉密人员对商业秘密的知悉范围：

- a) 员工磁卡；
- b) 门禁卡；
- c) 密码锁；
- d) 系统账号；
- e) 申请审批。

6.6 秘密流转管理

6.6.1 企业保密办公室应委派专职人员负责管理商业秘密及其相应载体的流转档案。档案管理工作应包括商业秘密及相应载体的研发制作记录、存放保管记录、借阅管理记录、领取使用记录、人员交接记录、信息备份记录、载体销毁记录等。

6.6.2 商业秘密及相应载体的流转档案应包括商业秘密及相应载体的名称和内部代号、流转情况、接触人员姓名、流转日期、是否泄漏等内容，并由档案管理人员和流转过程中接触过商业秘密的相关人员共同签字确认。

6.6.3 商业秘密及相应载体的流转档案亦可通过企业内部网络系统进行实名认证管理，任何商业秘密及相应载体的流转记录皆应采取网络系统电子留痕的管理方式进行。

6.7 保密协议签订

6.7.1 企业保密办公室应协同人力资源管理部门与企业员工共同签订商业秘密保密协议，明确要求企业员工遵守保密制度和承担保密义务，保密协议原件应分别保管于保密办公室和人力资源管理部门。

6.7.2 在涉及商业秘密的商务活动中，企业保密办公室应协同相关业务部门与商务活动对方企业共同签订商业秘密保密协议，明确要求相关合作方及相关工作人员承担保密义务，保密协议原件应分别保管于保密办公室和相关业务部门。

6.7.3 需要签订商业秘密保密协议的涉及商业秘密的商务活动包括但不限于下列内容：

- a) 商业咨询；
- b) 商业谈判；
- c) 技术评审；
- d) 专家论证；
- e) 成果鉴定；
- f) 合作开发；
- g) 技术转让；
- h) 合资入股；
- i) 外部审计；
- j) 尽职调查；
- k) 清产核资；
- l) 外客访问。

6.7.4 商业秘密保密协议应包括但不限于下列内容：

- a) 协议双方名称；
- b) 保密的内容和范围；
- c) 保密双方的权利和义务；
- d) 保密期限；
- e) 违约责任；
- f) 争议解决；
- g) 协议签订日期。

6.8 竞业限制要求

6.8.1 企业保密办公室应协同人力资源管理部门与企业涉密员工共同签订竞业限制协议，明确要求涉密员工遵守保密制度和承担竞业限制义务，竞业限制协议原件应分别保管于保密办公室和人力资源管理部门。

6.8.2 竞业限制协议适用的企业涉密员工应包括高级管理人员、高级技术人员和其他知悉商业秘密的工作人员。

6.8.3 竞业限制协议应妥善处理商业秘密保护与员工自由择业、涉密人员的竞业限制与人才合理流动的关系，维护企业员工的合法权益。

6.8.4 竞业限制协议应包括但不限于下列内容：

- a) 协议双方名称；
- b) 协议双方的权利和义务；
- c) 竞业限制期限；
- d) 竞业限制补偿金数额；
- e) 生效条件；
- f) 违约责任；
- g) 争议解决；
- h) 协议签订日期。

6.9 外来访客限制

6.9.1 企业外部人员访问活动应被限制在企业公共开放区域，并被以明示方式要求遵守企业保密制度，未经许可不得擅自进入涉密工作区域。企业外部人员访问活动应登记备案，登记内容应包括但不限于外部访问人员的个人信息、工作单位、访问时间、联系方式、访问目的、活动范围等内容。

6.9.2 企业外部人员访问确需进入涉密工作区域时，应另行签署保密协议，并在保密办公室及相关业务部门的工作人员陪同下进行访问活动。企业外部人员访问涉密工作区域期间，应被明确要求禁止实施录音、录像、摄影、信息存储等可能导致商业秘密泄露的行为。企业外部访问人员持有的具有录音、录像、摄影、信息存储等功能的电子设备应按企业保密办公室的要求统一管理，并在访问结束后予以返还。

6.10 涉密审查前置

6.10.1 企业保密办公室应建立涉密审查前置程序，对于企业业务部门或者企业员工计划实施的可能涉及商业秘密披露的行为主动适用涉密审查前置程序。未经涉密审查前置程序审核通过，任何可能涉及商业秘密披露的行为均不得实施。

6.10.2 企业涉密审查前置程序应适用于如下可能涉及商业秘密披露的行为，包括但不限于：产品宣传、技术推广、工艺演示、展会参展、学术会议、技术讲座、商务演讲、专利申请、论文发表、著作出版、新闻报道、设备维修、机器拆卸等。

6.10.3 企业保密办公室可以在涉密审查前置程序结束后作出如下决定：准许实施、脱密处理后实施、脱密处理后再次审查、不得实施。企业保密办公室应将审查决定通知相关业务部门和具体工作人员，相关业务部门负责人和具体工作人员应签字确认其知悉情况并承诺遵守审查决定。

6.11 保密业务培训

6.11.1 企业保密办公室应组织开展下列商业秘密保护培训：

- a) 新入职员工保密培训；
- b) 全体员工定期业务保密培训；
- c) 重点岗位、重要涉密人员定期专项保密培训；
- d) 离职、转岗、退休人员脱密保密培训。

6.11.2 在商业秘密保护培训后，企业保密办公室应要求企业员工签字确认其参加保密业务培训的情况并承诺遵守企业保密规定。

6.11.3 保密培训应实现下列目标：

- a) 使企业员工熟悉商业秘密保护制度和保护手册的具体规定，知晓商业秘密保护的权利和义务，增强商业秘密保护的责任意识；

- b) 使企业员工知晓企业商业秘密管理组织体系、商业秘密保护制度体系、商业秘密风险防范体系的构建和运作；
- c) 使企业员工能够按照商业秘密保护要求自觉规范行为方式，逐渐形成良好的企业商业秘密保护环境；
- d) 使企业员工知晓商业秘密侵权的行为类型，以便主动防范和避免商业秘密侵权行为的发生；
- e) 其他需要企业员工通过培训提升保密知识水平和保密能力的事项。

6.12 巡视检查

6.12.1 企业保密办公室应协同相关业务部门定期巡视检查企业商业秘密保护制度和保密措施的贯彻落实情况，以及商业秘密防护设施和监控设施的运行情况，对于巡视检查过程中发现的问题应予以及时纠正和解决。

6.12.2 企业保密办公室应将巡视检查的详细情况及改进建议形成书面报告，并提交企业商业秘密管理决策机构审阅和决定。企业保密办公室应将巡视检查报告存档备案，并根据商业秘密管理决策机构的决定落实改进措施。

6.12.3 企业保密办公室制作的定期巡视检查报告应包括以下内容：企业商业秘密保护制度现状、制度落实情况、制度有效性评价、制度改进措施等。

6.13 责任追究

6.13.1 企业保密办公室在定期巡视检查过程中以及通过其他渠道发现企业员工存在违反保密规定的行为，应根据企业商业秘密保护制度、企业员工商业秘密保护手册和相关法律规定提出初步处理意见，并提请企业商业秘密管理决策机构核准。

6.13.2 企业商业秘密管理决策机构认为企业员工违反保密规定的行为属于情节轻微，未给企业造成损失，宜根据企业处分规定予以处理的，应交由企业保密办公室协同人力资源部门执行处分决定。

6.13.3 企业商业秘密管理决策机构认为企业员工违反保密规定的行为属于情节严重，已给企业造成较大损失，可以根据相关法律规定通过法律救济方式处理的，应交由企业保密办公室协同法务部门按照法律规定处理。

7 风险防范

7.1 基本要求

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。

7.2 风险监测

7.2.1 企业保密办公室应建立风险监测机制，全面收集和系统分析可能对商业秘密保护构成现实风险或者潜在风险的信息。

7.2.2 企业保密办公室应建立商业秘密保护风险监测台账，对影响商业秘密保护的风险来源、风险类型、风险形成原因、风险发生后果、风险发生概率等因素进行系统地分析、统计、记录，为风险评估、风险预警和风险应对提供基础数据和分析参考。

7.2.3 企业商业秘密保护监测机制应由下列部分构成：内部管理监测、外部市场监测、行政处罚监测、司法审判监测等部分构成。具体情况如下：

- a) 内部管理监测：是指通过企业内部日常保密管理、定期巡视检查、企业员工举报等方式持续监测本企业商业秘密是否存在被侵犯的潜在风险或现实风险；
- b) 外部市场监测：是指通过企业外部客户监测、商业交易监测、竞争对手监测、同类产品或服务监测等方式持续监测本企业商业秘密是否存在被侵犯的潜在风险或现实风险；
- c) 行政处罚监测：是指通过市场监督管理部门发布的案件情况和处罚信息等渠道持续监测本企业商业秘密是否存在类似被侵犯的潜在风险或现实风险；
- d) 司法审判监测：是通过中国裁判文书网或各级法院官方网站发布的案件情况和判决信息等渠道持续监测本企业商业秘密是否存在类似被侵犯的潜在风险或现实风险。

7.3 风险评估

7.3.1 企业保密办公室应建立风险评估机制，对于商业秘密风险监测发现的潜在风险和现实风险可能给企业生产经营造成的负面影响和经济损失进行全面分析和系统评估，并制作风险评估报告。

7.3.2 企业保密办公室应建立风险评估量化标准，对商业秘密本身的商业价值和研发成本，商业秘密保护风险可能给企业经济利益、竞争优势、市场地位等方面造成的损失和影响做出全面和细致的评估。

7.3.3 企业保密办公室经过风险评估后认为商业秘密保护风险较小，通过现有的商业秘密保护措施能够将安全风险消除的，可以自行决定风险处理方案，但应报请商业秘密管理决策机构备案。

7.3.4 企业保密办公室经过风险评估后认为商业秘密保护风险较大，需要通过制定新的商业秘密保护措施、采取外部应对措施或者法律救济措施等方式应对的，应及时启动风险预警机制。

7.4 风险预警

7.4.1 企业保密办公室应建立风险预警机制，对于经商业秘密风险评估确定的较大安全风险应及时发出风险预警，并制作风险预警报告。

7.4.2 企业保密办公室可以根据安全风险的严重性和迫切度，将商业秘密保护风险预警的级别分为风险蓝色预警、风险橙色预警、风险红色预警等由低到高三个预警级别，并根据风险预警级别制定相应的风险应对方案。

7.4.3 企业保密办公室在判定商业秘密保护安全风险的严重性和迫切度时，应综合考虑下列因素：

- a) 商业秘密的性质；
- b) 商业秘密的企业内部等级；
- c) 商业秘密的商业价值；
- d) 商业秘密的研发成本；
- e) 商业秘密泄露可能造成的损失和影响；
- f) 商业秘密泄露或被侵犯的紧迫程度。

7.4.4 企业保密办公室应将商业秘密保护的风险预警报告和风险评估报告及时送交企业商业秘密管理决策机构，并由管理决策机构决定是否启动风险应对机制。

7.5 风险应对

7.5.1 企业保密办公室应建立风险应对机制，对于已经发出风险预警的商业秘密保护问题，按照商业秘密管理决策机构讨论决定的风险应对方案及时采取风险应对措施。风险应对方案应明确规定方案实施部门、具体负责人、实施时间、实施计划、应对措施、预期结果等。

7.5.2 企业保密办公室宜根据实际情况采取如下风险应对措施：企业内部应对措施、外部市场应对措施、法律救济应对措施等。具体情况如下：

- a) 企业内部应对措施，是指通过完善或者革新企业商业秘密保护制度和保护措施，消除商业秘密保护的现实风险或者潜在风险；
- b) 外部市场应对措施，是指通过商业谈判、商业交易等市场经济运作方式，挽救已经被他人获取但尚未披露的商业秘密，进而消除商业秘密保护的现实风险或者潜在风险；
- c) 法律救济应对措施，是指通过行政机关和司法机关提供的行政救济、民事救济、刑事救济等方式，消除商业秘密保护的现实风险或潜在风险，维护商业秘密权利人的权利，弥补商业秘密权利人的损失。

8 评价与持续改进

根据前述商业秘密基本原则以及检查、分析的结果，定期持续改进商业秘密保护体系，制定和落实改进方案与措施。
