|  |  |
| --- | --- |
| ICS  | 03.100.01 |
| CCS  | A 01 |

|  |
| --- |
|  46 |

海南省地方标准

DB 46/T XXXX—XXXX

商业秘密保护管理和服务规范

Management and service specifications for protection of trade secrets

2022 - XX - XX发布

2022 - XX - XX实施

海南省市场监督管理局  发布

目次

[前言 III](#_Toc113467549)

[1 范围 1](#_Toc113467550)

[2 规范性引用文件 1](#_Toc113467551)

[3 术语和定义 1](#_Toc113467552)

[4 基本要求 2](#_Toc113467561)

[4.1 机构和人员 2](#_Toc113467562)

[4.2 保密措施 2](#_Toc113467563)

[5 人员管理 3](#_Toc113467564)

[5.1 涉密员工 3](#_Toc113467565)

[5.2 来访人员 4](#_Toc113467566)

[5.3 其他人员 4](#_Toc113467567)

[6 涉密区域管理 4](#_Toc113467568)

[7 涉密信息管理 5](#_Toc113467569)

[7.1 信息处置 5](#_Toc113467570)

[7.2 涉密信息管理 6](#_Toc113467571)

[7.3 对外合作 8](#_Toc113467572)

[8 检查和改进 8](#_Toc113467573)

[9 维权 8](#_Toc113467574)

[9.1 应急处置 8](#_Toc113467575)

[9.2 证据收集 9](#_Toc113467576)

[9.3 维权途径 9](#_Toc113467577)

[10 服务 9](#_Toc113467578)

[10.1 政府管理服务部门 9](#_Toc113467579)

[10.2 第三方社会服务机构 9](#_Toc113467580)

[10.3 园区服务平台 10](#_Toc113467581)

[附录A （资料性） 商业秘密的保护范围 12](#_Toc113467582)

[A.1 技术信息 12](#_Toc113467583)

[A.2 经营信息 12](#_Toc113467584)

1. 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由海南省市场监督管理局提出并归口。

本文件起草单位： 海南省质量技术监督标准与信息所、海南省标准化协会。

本文件主要起草人：李伟、王小英、黄家将、孙林芳、李廷秀、金佳佳、梅姬、吴清宇。

商业秘密保护管理和服务规范

* 1. 范围

本文件规定了商业秘密保护的基本要求、人员管理、涉密区域管理、涉密信息管理、检查和改进、维权及服务等内容。

本文件适用于企业商业秘密的保护管理工作，以及园区、经济开发区、特色小镇、行业协会、第三方社会服务机构的商业秘密保护服务。

* 1. 规范性引用文件

本文件没有规范性引用文件。

* 1. 术语和定义

下列术语和定义适用于本文件。

* + 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。

1. “不为公众所知悉”、“具有商业价值”和“相应保密措施”的具体内容见《中华人民共和国反不正当竞争法》、《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》等有关法律法规、司法解释的规定。
	* 1.

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。

* + 1.

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。

1. 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。
	* 1.

涉密载体 secret-related carriers

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，包括磁性介质、光盘、U盘、硬盘、服务器等电子存储介质（即涉密存储介质）和纸质材料（即涉密纸质文档）。

涉密物品 secret items

含有商业秘密信息的设备和产品。

* 1. 基本要求
		1. 机构和人员
			1. 应由企业的高级管理人员统筹管理商业秘密保护工作，宜设立专门机构或依托相关部门开展商业秘密保护工作。
			2. 应配备专(兼)职保密员，宜在涉及商业秘密保护的重点部门配备兼职保密员。
			3. 商业秘密保护部门和保密员应履行包括但不限于以下职责：
1. 负责商业秘密保护相关制度的建立、实施、检查及改进；
2. 组织相关部门做好商业秘密的识别、定密及日常登记与管理；
3. 组织相关部门制定适宜的保密措施；
4. 组织企业员工进行商业秘密保护培训；
5. 负责涉嫌侵犯商业秘密行为、涉嫌侵犯商业秘密罪案件的证据的整理、搜集、举证、协助调查取证等维权工作。
	* 1. 保密措施
			1. 应制定商业秘密保护管理制度、培训制度和奖惩制度。可根据企业规模和实际业务需求制定下列制度：
6. 涉密文件管理的制度；
7. 涉密物品管理的制度；
8. 涉密计算机账户、数据管理的制度；
9. 涉密场所管理的制度；
10. 涉密人员管理的制度；
11. 外来人员保密的制度；
12. 合作单位保密的制度；
13. 客户信息保密的制度；
14. 考核评级制度；
15. 网上处理机制等。
	* + 1. 应分析确定商业秘密保护的重点部门和重点岗位，可划定商业秘密保护重点区域，宜实行物理隔离保护。
			2. 参照附录A确定商业秘密的保护范围，宜以发文形式公布。
			3. 应在合同条款中规定商业秘密保护要求，或与合作单位单独签订商业秘密保护合同/协议。
			4. 一般性的保密措施应符合下列保密要求：
16. 限制了接触范围；
17. 明确了接触的准许条件或者采取了限制接触的技术手段；
18. 对接触人员明确赋予了未经授权不得使用、披露的义务；
19. 接触到商业秘密的人员都能显然识别和认识到其为商业秘密。
	1. 人员管理
		1. 涉密员工
			1. 入职

应对拟入职涉密岗位人员进行保密事项提醒，告知其有保护企业商业秘密的义务，并提醒其不得泄露前雇主的商业秘密。

新入职涉密岗位人员（含转岗）应签订商业秘密保护合同/协议，明确约定保密范围和期限，双方的权利和义务以及违约责任等。

涉密重点岗位员工入职前宜做背景调查。根据需要，可对部分高级管理人员、高级技术人员开展入职前核查，包括查验犯罪记录。

* + - 1. 宣传培训

应对新入职员工进行保密培训，以确保其：

1. 理解商业秘密权利、义务，树立保密意识；
2. 理解企业商业秘密管理相关规定；
3. 理解其岗位的保密责任。

制定年度计划，采取集中培训、发放资料、网络培训等方式开展年度常态化商业秘密保护宣传及培训。

宜对签订商业秘密保护合同/协议的人员进行保密考核，考核结果存档。

* + - 1. 日常管理

应遵守企业商业秘密保护制度，做好本岗位商业秘密保护工作，包括：

1. 涉密信息及载体应及时上报，由保密员归档统一管理；
2. 使用涉密信息应履行登记手续；
3. 涉密电子文档、数据按规定途径和要求使用、流转等；
4. 离开工作岗位前及时下线工作账户，或设置电脑锁屏等。

未经商业秘密保护部门审批，不应出现下列行为：

1. 登陆未授权账户；
2. 超范围使用涉密文件资料、物品、数据；
3. 复制、发送涉密电子文档；
4. 将涉密电子文档存于未授权载体或网络空间；
5. 拍摄、摘抄涉密资料；
6. 拍摄、测绘、仿造涉密物品；
7. 进入非授权涉密区域；
8. 披露企业未公开的信息等。

中高层管理人员和涉密重要岗位员工不应出现下列行为：

1. 兼职或入股与所在企业经营相关、相同或相似的企业；
2. 同与所在企业有交易关系、竞争关系、行业相同或相似的国内外企业进行涉密交易；
3. 组建、参与组建或变相投资与所在企业经营相关相同或相似的企业。
	* + 1. 离职

涉密岗位员工离职前，宜采取适当措施进行脱密。

离职员工应主动移交一切涉密载体和物品，包含但不限于：

1. 涉密文件资料、数据及其载体、物品；
2. 账户信息：如账号、密码；
3. 工作电脑；
4. 门禁卡等。

可进行离职检查，检查内容为：

1. 检查工作电脑数据是否完整；
2. 检查工作账户近期是否有异常操作，如异常查询、下载、拷贝、修改、删除等；邮箱邮件收发记录；
3. 离职前一定期限内的涉密文档、数据的查阅和使用情况等。

宜进行离职谈话，告知离职员工不应：

1. 复制、带离、损毁、纂改、拍摄涉密文件资料、物品；
2. 查阅、拷贝、纂改、发送涉密电子文档、数据；
3. 删除、更改账户；
4. 披露、使用商业秘密等。

高级技术人员、高级管理人员及其他负有保密义务的人员（如职业经理人、技术、采购、销售等涉密重点岗位人员）可签订竞业限制协议等商业秘密保护确认文书，并掌握离职员工在竞业限制期限内的任职情况。

及时通知与离职员工有关的供应商、客户、合作单位等，做好业务交接。

* + 1. 来访人员
			1. 来访人员进入涉密区域应经审批，履行进出登记，佩戴临时证件。
			2. 来访人员进入涉密区域，受访部门应安排人员陪同，限制来访者使用具有录音、摄像、拍照、信息存储等功能的设备。
		2. 其他人员
			1. 与供应商、客户、合作方签订保密协议，约定保密内容和范围、保密责任和义务及违约责任。
			2. 聘任或委托的外聘专家、顾问、翻译、律师等可能接触涉密信息的外部人员，宜做背景调查，并签署限制性条款或协议。
			3. 涉及商业秘密的会议或其他活动，应采取下列保密措施：
1. 选择具有保密条件的场所；
2. 根据工作需要，限定参加人员的范围，指定参与涉密事项的人员；
3. 告知参加人员保密要求，必要时签订保密承诺书；
4. 通过拍照、摄像等方式做好记录。
	1. 涉密区域管理

企业应识别涉密区域，门口张贴涉密区域标志。宜将下列部门或地点列为涉密重点区域：

1. 研发设计、信息管理、财务等部门；
2. 控制中心、服务器机房等；
3. 涉密档案、涉密载体存放地点；
4. 未公开的样品存放地点；
5. 模具、专用夹具、重要零部件等的存放区；
6. 重要原材料、重要半成品等保密物资存放区等。

涉密区域限制外来人员访问、参观、考察，确因工作需要进入涉密区域应按5.2进行管理。

涉密重点区域实行进出登记和保密告知，应有保护措施：

1. 划定相对独立的空间，进出口有涉密区域标识；
2. 设有门禁隔离设施，涉密区域进入需获得许可；
3. 进出口处设置报警装置，非法闯入能立即告警；
4. 限制使用具有录音、摄像、拍照、信息存储等功能的设备；
5. 必要时采取网络隔离阻断等。

宜在涉密区域内设置画报、标语等，营造商业秘密保护氛围。

* 1. 涉密信息管理
		1. 信息处置
			1. 定密

参照附录A的范围，确定商业秘密内容并按重要性实行分级管理，一般分为绝密、机密和秘密三个等级，定密结果应由分管负责人审批。

下列可认定为公众所知悉的信息不应作为企业保护的商业秘密：

1. 在所属领域属于一般常识或者行业惯例的；
2. 仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；
3. 已经在公开出版物或者其他媒体上公开披露的；
4. 已通过公开的报告会、展览等方式公开的；
5. 所属领域的相关人员从其他公开渠道可以获得该信息的。
6. 公知信息和基础理论；
7. 已申请并公开的专利；
8. 企业以其他方式公开的信息；
9. 可通过合法渠道获得的信息；
10. 法律法规规定的其他情形。
	* + 1. 解密

企业认为不需要继续保密的信息可予以解密，可采取的解密方式为：

1. 移出涉密区域；
2. 消除或涂改密级标识、提示；
3. 电子文档解密；
4. 发文公布等。
	* + 1. 隐密

下列情形涉及商业秘密信息时，应予隐密：

1. 尽职调查时；
2. 与供应商、客户、合作方等的沟通和信息往来中；
3. 信息公开、发布、流转时。

可采取的隐密方式为：

1. 隐藏或删除涉密信息；
2. 对涉密信息进行模糊化处理等。
	* + 1. 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，经商业秘密保护部门审批后实施。

可采取下列方式对销毁过程进行监督管理：

1. 在视频监控范围内销毁；
2. 不少于2 名员工见证下销毁；
3. 对销毁过程录像等。

应采取合适的方式妥善销毁：

1. 文件、资料应粉碎成颗粒状或焚烧处置；
2. 电子信息应利用彻底删除软件永久删除；
3. 其他合适的方式。
	* 1. 涉密信息管理
			1. 涉密信息分类

按涉密信息的存在形式分为纸质文件和资料、账户和电子信息、涉密载体和物品。

* + - 1. 涉密文件、资料管理

应有密级、保护期限等标识，归档存放。

由部门专兼职保密员登记造册，按权限使用，查阅、借阅、续借应履行登记手续。

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。

新闻发布、论文发表、专利申请等信息发布和公开时，应由商业秘密保护部门对信息进行审核。

销毁正式发布的文件（含复制文件），应经商业秘密保护部门、法定代表人或其授权人审批。参照7.1.4执行。

* + - 1. 涉密账户、电子信息管理
				1. 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：

1. 合理分配不同层级账户的功能和审批权限；
2. 合理分配项目中不同账户的功能和使用期限；
3. 合理设定不同账户的访问、操作、查看等权限及其使用期限；
4. 合理设定不同账户的互联网使用权限。

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。

* + - * 1. 口令管理

各类设备、数据库和应用系统应设有账户和密码，不应使用默认密码，不应保存密码自动登陆。

根据企业的业务类型，采取适当的账户、密码管理方式，如：

1. 限制使用简单密码；
2. 必要时定期或不定期更改密码；
3. 输错密码一定次数锁定账户。
	* + - 1. 电子信息保护

涉密数据应存储于企业授权的存储设备和应用系统，不得存储于非授权存储设备、网络空间。机密、绝密数据应采用加密方式存储。

指定专人进行解密操作，员工按照权限使用加密数据。

员工超出权限需要查阅或使用加密数据的，应经商业秘密保护部门批准，在查阅或使用完成后，予以删除，不应非因工作需要而擅自使用。

宜在各类场景进行保密义务提醒，如：

1. 在账户登陆提示、账户登陆后的主界面设置保密义务提醒。
2. 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；
3. 在涉密音视频开头提示保密义务。

应定期对涉密数据进行备份，妥善保存备份数据。

* + - * 1. 电子信息流转

收发涉密数据应使用唯一出入口，不得流转至不相关的人员或系统。

内部局域网应与互联网隔离，涉密数据网上传递应通过内部局域网或加密的互联网通道完成。

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

对外发送涉密数据应采取加密措施，数据发送与密钥发送不应采用同一途径。

应对涉密数据拷贝采取限制措施，经审核批准后方可拷贝，妥善保存拷贝记录。

应与客户、合作单位等涉密数据接收单位签订保密协议。

* + - * 1. 安全防范

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，可实时报告异常入侵、登陆、获取信息的行为。

* + - 1. 涉密载体、物品管理

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。

涉密载体、物品的存放地点宜设为涉密重点区域，宜采取物理隔离的方式进行保护。

未经商业秘密保护部门、法定代表人或其授权人审批，不得拍摄、测绘或仿造。

由部门专兼职保密员登记造册，按权限使用，领用应履行登记手续。

跨区域转移应履行审批手续，必要时采取防护措施。

* + 1. 对外合作
			1. 商务活动

采购、销售、委托开发、委托生产、参展等商务活动时应注意：

1. 开始商务谈判前或提供涉密信息前，应与对方签署保密协议；
2. 参展过程中通过隐密、与展览方签订保密协议等方式降低泄密风险；
3. 对协议履行过程中涉密信息的使用情况和泄密情况进行监督管理，保留证据。
	* + 1. 技术合作

技术合作中应调查合作方的商业秘密管理能力，优先选择商业秘密管理能力强的合作方。

* 1. 检查和改进

应开展商业秘密保护管理情况检查，检查内容包括但不限于：

1. 商业秘密保护制度建立情况；
2. 涉密人员管理情况；
3. 涉密区域管理情况；
4. 商业秘密的定密、解密、脱密、隐秘情况；
5. 涉密文件、资料的管理情况；
6. 涉密账户、电子信息的管理情况；
7. 涉密载体、物品的管理情况。

在检查过程中，发现有泄密情况及隐患的，应及时采取纠正、预防措施。

* 1. 维权
		1. 应急处置
			1. 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。
			2. 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。
			3. 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. 采取措施，将危害和损失控制在最小限度内等；
3. 启动对商业秘密泄露的核查、确认和评估，查明原因、责任人。
	* 1. 证据收集

企业发现商业秘密被侵犯的迹象、线索时，应及时与管辖地的商业秘密保护服务机构、市场监督管理部门等联系，在其指导下搜集下列证据，必要时进行证据保全公证：

1. 泄密信息的具体内容、载体，企业已采取的保护措施；
2. 泄密信息为一般公众不知悉或者无法轻易获得的信息；
3. 可能的泄密途径；
4. 可能与泄密信息有关的人员（如在职员工、离职员工、退休员工）的信息：在本企业的工作经历、工作内容、接触到的涉密信息，在本企业接受保密培训的记录，与企业签订的商业秘密保护合同/协议。
5. 可能与泄密信息有关的第三方等；
6. 侵犯涉密信息的具体行为表现；
7. 对方使用泄密信息发生侵权可能导致的后果。
	* 1. 维权途径
			1. 根据证据收集情况，企业可依法采取下列方式进行维权：
8. 向市场监督管理部门举报；
9. 申请劳动仲裁或商事仲裁；
10. 向人民法院提起民事诉讼；
11. 向公安机关报案。
	* + 1. 涉及国家秘密的，应向国家安全部门报告。
	1. 服务
		1. 政府管理服务部门
			1. 相关部门应加大对互联网、大数据、区块链、云计算、人工智能、新一代信息技术、石油化工新材料、现代生物医药、南繁育种、深海科技、航天科技等行业商业秘密保护指导。
			2. 中医药、老字号、非物质文化遗产、传统知识、民间文艺和少数民族文化等知识产权的创造和保护提供指导、咨询等服务。
			3. 引导知识产权相关权利人利用商业秘密保护等方式和保护规则维护合法利益。
			4. 相关部门按《海南自由贸易港知识产权保护条例》打击侵犯商业秘密的行为。
		2. 第三方社会服务机构

鼓励第三方社会服务机构开展商业秘密保护服务，包括但不限于：

1. 开展商业秘密培训；
2. 提供商业秘密专业知识咨询；
3. 协助企业建立商业秘密保护机制；
4. 开发和维护涉密文件、数据的信息管理系统；
5. 协助被侵权企业收集证据和协助维权等。
	* 1. 园区服务平台
			1. 平台建设

优势产业集聚的园区、经济开发区、特色小镇、行业协会等，可根据自身力量和企业需求，设立涵盖商业秘密保护的服务平台，为辖区企业快速审查、快速确权、快速维权等商业秘密保护服务。

* + - 1. 工作机构

应合理设置岗位，配置商业秘密保护专（兼）职工作人员，建立工作人员管理制度，明确工作职责，并签订保密协议，保障服务平台正常运营。

宜吸引商业秘密保护专家团队、调解机构、律师事务所等第三方社会组织和人员，聚集、整合服务资源。

可协调下列商业秘密保护相关部门在园区设立服务指导站：

1. 市场监督管理部门；
2. 公安机关、检察院、法院等；
3. 仲裁机构等。

宜设独立的商业秘密保护服务窗口，也可依托园区知识产权保护服务窗口提供服务。

* + - 1. 服务内容
				1. 宣传培训

应开展辖区商业秘密保护宣传，可采取的方式为：

1. 定期举办商业秘密保护培训班；
2. 编制、印发商业秘密保护宣传资料；
3. 利用园区媒体平台宣传等。

可组织适合企业不同层次人员的商业秘密保护专题培训：

1. 对企业法定代表人、股东、高级管理人员开展商业秘密保护重要性和必要性培训；
2. 对企业从事商业秘密保护工作的专兼职人员开展商业秘密保护实务及案例培训；
3. 对企业商业秘密保护重点岗位人员开展商业秘密保护意识培训；
4. 对企业员工开展商业秘密保护知识普及培训。
5. 利用行业协会、学会、商会等渠道将维权成功的案例向企业广泛宣传。
	* + - 1. 指导服务

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。

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。

引导园区企业建立和完善商业秘密保护工作体系，包括但不限于：

1. 界定商业秘密保护范围；
2. 建立和完善商业秘密保密制度；
3. 建立和完善商业秘密分类管理制度；
4. 建立和完善商业秘密使用管理制度；
5. 建立和完善商业秘密保护的应急反应机制。
	* + - 1. 维权协助

当企业商业秘密涉嫌被侵权，向园区平台申请协助时，应协助企业搜集、整理维权材料。

根据被侵权企业提供的材料，引导企业采取下列合理的维权途径：

1. 向市场监督管理部门举报；
2. 申请劳动仲裁或商事仲裁；
3. 向人民法院提起民事诉讼；
4. 向公安机关报案。

依据被侵权企业的意愿，协助执法部门开展泄密核查、现场检查及案件查处等，并协助做好调解服务。

配合市场监督管理部门、仲裁机构、法院等部门化解争议。

1.
2. （资料性）
商业秘密的保护范围
	1. 技术信息

商业秘密的技术信息保护范围见表A.1。

* 1. 涉密技术信息

|  |  |
| --- | --- |
| 项 目 | 表现形式 |
| 设计信息 | 设计图及其草案、模型、样板、设计方案、测试记录及数据等。 |
| 采购技术信息 | 型号、牌号、定制品技术参数等。 |
| 生产信息 | 产品的配方、工艺流程、工艺参数、作业指导书等。 |
| 设备设施信息 | 涉密生产设备、仪器、夹具、模具等中的技术信息。 |
| 软件程序 | 设计计划、设计方案、源代码、应用程序、电子数据等。 |
| 其他 | 企业认为有必要采取保密措施其他技术信息，如未公开的专利申报信息等。  |

* 1. 经营信息

商业秘密的经营信息保护范围见表A.2。

* 1. 涉密经营信息

|  |  |
| --- | --- |
| 项 目 | 表现形式 |
| 管理文件 | 文件、规章制度等。 |
| 决策信息 | 战略决策、管理方法等。 |
| 研发信息 | 研发策略、研发经费预算等 |
| 采购经营信息 | 采购渠道、采购价格、采购计划、采购记录等。 |
| 营销信息 | 营销策划、营销方案、营销政策、营销手册等。 |
| 招投标信息 | 标书、标底等。 |
| 财务信息 | 财务报表、财务分析、统计报表、预决算报告、各类帐册、工资信息等。 |
| 供应商和客户信息 | 名称、联系人、联系方式、交易习惯、合同内容、交提货方式、款项结算等。 |
| 销售信息 | 销售记录、销售协议等。 |
| 其他 | 企业认为有必要采取保密措施其他经营信息。 |

