ICS 03.100.20
CCS A 10

DB12

天 津 市 地 方 标 准

DB12/T 1439—2025

商业秘密保护管理和服务规范

Management and service specification for trade secret protection

2025－02－12 发布　　2025－03－15 实施

天津市市场监督管理委员会　　发 布

目　　次

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。

本文件由天津市市场监督管理委员会提出并归口。

本文件起草单位：天津市市场监督管理委员会、天津市滨海新区市场监督管理局、天津滨海高新技术产业开发区市场监督管理局。

本文件主要起草人：庄健、毕思友、陈洪波、井翠霞、王兵、王思予、李桢、郭敏。

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原则、商业秘密的范围、企业自主保护与管理、维权及服务等内容。

本文件适用于企业开展商业秘密保护管理和服务工作，其他组织可参照执行。

2 规范性引用文件

本文件没有规范性引用文件。

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

涉密人员 secret-related person

根据工作职责或者保密协议有权接触、使用、掌握商业秘密信息的企业员工或其他人员。

3.3

涉密载体 secret-related carrie

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各类介质，如纸介质、电磁介质、光介质等。

3.4

涉密物品 secret-related item

含有商业秘密信息的设备和产品，如计算机、手机、原材料、成品、半成品、样品等。

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，如车间、研发室、实验室、机房、保密室、档案室等。

4 基本原则

商业秘密保护首先是权利人的自主保护，实施保护的商业秘密由权利人自主提出，确定的商业秘密应具备秘密性、价值性和保密性。商业秘密保护应遵循重在预防、主动维权、协同保护的原则，建立自主保护、行政保护与司法保护一体的商业秘密保护体系。

5 商业秘密范围

5.1　企业应根据自身情况界定商业秘密的范围，商业秘密一般分为技术信息和经营信息。

5.2　技术信息指与技术有关的结构、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。

5.3　经营信息是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。

6　企业自主保护与管理

6.1　组织机构

6.1.1　企业的最高管理者应具备商业秘密保护意识，商业秘密管理工作应由最高管理者牵头进行。

6.1.2　企业可设立商业秘密保护部门或依托相关部门开展商业秘密保护工作，配备专（兼）职保密人员。

6.1.3　商业秘密保护部门和保密人员应履行包括但不限于以下职责：

——建立和实施商业秘密保护有关制度；

——识别和管理商业秘密事项，如涉密人员、涉密载体、涉密物品、涉密区域等；

——组织制定、实施商业秘密保护措施；

——组织商业秘密保护宣传、培训、考核；

——监督、检查商业秘密保护管理工作的落实和执行；

——处理泄密或侵犯商业秘密事件；

——商业秘密保护管理制度进行评估和改进。

6.2　秘密管理

6.2.1　企业应对确定的商业秘密进行分类分级，并按照密级高低实行分级保护和管理。

6.2.2　企业应建立商业秘密保护清单，并对商业秘密进行标识。

6.2.3　企业应明确商业秘密的保密事项，并建立对涉密人员、涉密载体、涉密物品、涉密区域、涉密商务活动等事项的管理要求，采取相应的保密措施。

6.2.4　企业应根据实际业务和经营情况制定商业秘密保护管理制度并在企业内部公开，内容包括但不限于：

——商业秘密识别与分级管理制度；

——涉密人员管理制度；

——涉密载体管理制度；

——涉密物品管理制度；

——涉密区域管理制度；

——涉密商务活动管理制度；

——涉密信息管理制度；

——应急管理制度；

——检查和改进制度；

——奖惩管理制度。

6.2.5　商业秘密保护的具体管理内容和措施参见附录 A。

6.3　应急管理

6.3.1　企业应制定商业秘密泄密或侵权的应急处理预案，预案内容包括但不限于：

——应急小组成员及职责；
——紧急应对流程；
——泄密或侵权溯源和评估定级方案；
——防止信息进一步扩散、危害和损失扩大的应急措施方案；
——维权方案；
——总结和改进方案。

6.3.2 应急小组一般由商业秘密保护部门或企业高级管理人员牵头，成员可包括人事部门、法务部门、信息技术部门、行政部门、公关部门等。

6.3.3 紧急应对流程一般包括事件上报、成立应急小组、核查确认泄密或侵权内容、评估泄密或侵权事件等级、应急处置、维权和责任追究、形成事件报告、提出整改方案等。

6.3.4 对泄密或侵权事件的评估定级，可考虑如下因素：
——涉及的商业秘密等级和数量；
——侵权的方式，如未经许可的复制、向第三方披露、被公开、被第三方使用；
——事件对企业造成的影响；
——泄密或侵权嫌疑人的情况；
——其他影响泄密或侵权事件评估分级的因素。

6.3.5 出现商业秘密泄露的征兆或者迹象时，企业应采取措施防止信息扩散，将危害和损失控制在最小限度内。措施包括但不限于：
——涉密载体、物品等失窃或被未经许可复制的，应做好现场保护工作，调查并确定泄密范围和流向，及时追回被窃涉密载体、物品或复制后的版本；
——商业秘密被上传至信息系统、互联网或其他未被允许渠道公开的，应联系相应渠道的运营方或信息管理部门对泄露信息进行屏蔽或删除；
——向侵权嫌疑人发送侵权告知函，要求其立即停止侵权行为；
——向法院申请保全措施。

6.3.6 企业应加强对员工的培训和引导，使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。

6.3.7 企业可以定期进行商业秘密泄密应急处理演练，提高应对商业秘密泄密情形发生时的处置能力。

6.4 检查评估与改进

6.4.1 检查评估

6.4.1.1 企业应对商业秘密保护管理情况进行监督检查，确保其持续的适宜性、充分性和有效性。

6.4.1.2 企业的商业秘密保护部门或实际开展商业秘密保护工作的相关部门应制定监督检查方案，内容应包括但不限于：
——监督检查工作的内容和方法；
——监督检查工作的职责和权限；
——执行监督检查的频次和时限；
——监督检查结果运用的整改、问责、奖惩机制。

6.4.1.3 监督检查内容应包括但不限于：
——商业秘密的定密、分级、流转；
——涉密人员管理情况；
——涉密载体管理情况；
——涉密物品管理情况；

——涉密区域管理情况；
——涉密商务活动管理情况；
——操作系统、办公软件、信息系统等工具软件的账号、权限、密码管理和使用商业秘密情况；
——商业秘密保护管理制度建立和实施情况。

6.4.1.4 监督检查方法可包括但不限于：
——调取涉密载体、涉密物品、涉密信息使用记录；
——调取涉密区域出入口和内部监控；
——调取操作系统、办公软件、信息系统等工具软件的日志文件等；
——现场查验、问询涉密人员工作情况；
——调取涉密活动记录及附属合同等。

6.4.1.5 企业应根据监督检查结果评估商业秘密保护管理制度和措施的适宜性、充分性和有效性并形成评估结论或报告。

6.4.1.6 企业可委托第三方机构开展商业秘密保护监督检查与评估。

6.4.2 改进

6.4.2.1 企业应针对监督检查发现的问题制定整改计划，采取有效措施持续改进。

6.4.2.2 企业应对改进情况进行复查、复评。

7 维权

7.1 证据收集

7.1.1 企业应及时收集并固定以下证据材料，必要时可进行证据保全公证。

——商业秘密权属证明，包括但不限于以下内容：
- 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材料；
- 商业秘密交易转让合同或授权使用许可协议等证明材料。

——商业秘密的具体内容和载体；

——商业秘密不为公众所知悉的证明，包括但不限于下列情形：
- 该信息在所属领域不属于一般常识或者行业惯例；
- 该信息不仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员不能通过观察上市产品即可直接获得；
- 该信息未在公开版物或者其他媒体上公开披露；
- 该信息未通过公开的报告会、展览会等方式公开；
- 所属领域的相关人员无法从其他公开渠道获得该信息。

——商业秘密具有商业价值的证明，包括但不限于下列内容：
- 生产经营活动中形成的阶段性成果；
- 研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间。

——已对商业秘密采取相应保护措施的证明，包括但不限于下列情形：
- 签订保密协议或者在合同中约定保密义务；
- 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；
- 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；

- 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；
- 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；
- 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。

——可能与泄密信息有关的人员信息,包括但不限于以下内容：

- 有关人员在本单位的工作经历、工作内容、接触到的涉密信息以及其他有可能、有条件接触到商业秘密的证明材料；
- 有关人员在本单位接受保密培训的记录；
- 有关人员与本单位签订的保密协议。

——侵权信息与企业商业秘密相同或者实质相同的证明材料；

——侵犯商业秘密的具体行为表现；

——侵犯商业秘密行为导致的后果。

7.1.2 商业秘密的非公知性、同一性等专业技术事项可委托第三方机构进行鉴定。

7.2 维权途径

7.2.1 当商业秘密被侵犯时，企业应主动维权，根据实际情况可依法采取下列维权方式：

——和解与调解；

——寻求行政保护；

——申请商事仲裁；

——寻求司法保护。

7.2.2 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。

7.3 和解与调解

7.3.1 企业可以通过协商和解方式解决商业秘密侵权纠纷，在和解协议中可以约定一定的赔偿金额、保密义务等条款，也可以基于实际的商业谈判情况和具体的商业需求，在符合法律规定的情况下，约定竞业禁止等条款。

7.3.2 企业可以与侵权人双方本着真实自愿的原则委托共同认可的政府机构或社会机构进行调解或由人民法院委派调解机构进行诉前、诉中调解。

7.4 行政保护

7.4.1 企业可以向违法行为发生地的县级以上市场监督管理部门举报，应按照市场监督管理部门要求提供相应材料。

7.4.2 企业可根据案件进展情况，在立案后变更、增加其所主张的商业秘密具体内容。

7.4.3 经核查立案后，企业应积极配合市场监督管理部门进行询问、现场检查等调查取证工作。

7.5 商事仲裁

违反协议约定的保密义务并且约定商事仲裁管辖条款的，若尚未构成刑事犯罪的，应向约定的仲裁委员会申请仲裁。

7.6 司法保护

7.6.1 民事保护

7.6.1.1 商业秘密民事案件可向有管辖权的人民法院提起民事诉讼，并提供初步证据，证据内容可参照 7.1。

7.6.1.2 针对以下情形可以向人民检察院提请商业秘密诉讼活动法律监督：

——已经发生法律效力的民事判决、裁定、调解书符合《中华人民共和国民事诉讼法》第二百零九条第一款规定的；

——认为民事审判程序中审判人员存在违法行为的；

——认为民事执行活动存在违法情形的。

7.6.2 刑事保护

商业秘密侵权案件造成企业损失情况符合《最高人民检察院 公安部关于修改侵犯商业秘密刑事案件立案追诉标准的决定》的有关规定的，企业可向犯罪地的公安机关报案，由公安部门对侵权人进行刑事立案调查。企业应按照公安机关的要求提供相应材料。对公安机关应当立案而不予立案的，企业可到检察机关申请立案监督。

8 服务

8.1 概述

8.1.1 提供商业秘密保护服务的机构可以是行政管理部门、行业组织、第三方社会服务机构等。

8.1.2 服务机构可按照市场化原则，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，以设立涵盖商业秘密保护的服务平台等形式，提供宣传、培训、咨询、指导、快速维权等商业秘密保护服务。

8.1.3 提供商业秘密保护服务的相关人员应具备商业秘密保护的专业知识，能及时解决企业在商业秘密保护工作中发现的问题。

8.2 宣传

8.2.1 服务机构应对管理范围内的企业开展商业秘密保护宣传。

8.2.2 商业秘密保护宣传推广可通过制作宣传手册、派发宣传单张、拍摄宣传视频等形式，借助报刊杂志、新兴自媒体等载体，以“线上+线下”并行、“流动+定点”互补等方式进行。

8.2.3 可对具有社会影响力、示范意义较大的典型商业秘密保护案例开展专题宣传活动。

8.3 培训

8.3.1 服务机构应制定培训方案和计划，定期组织企业、服务机构工作人员开展商业秘密保护培训。

8.3.2 培训可采用多种形式开展，培训形式包括但不限于：

——发放培训资料；

——线下培训；

——在线培训；

——录课培训。

8.3.3 可对企业不同层次人员开展商业秘密保护专题培训：

——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；

——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；

——对企业员工开展商业秘密保护知识培训和警示教育。

8.3.4 对服务机构相关部门工作人员可开展商业秘密保护技能和服务意识提升培训。

8.4 保护指导与支持

8.4.1 服务机构可开展商业秘密保护指导工作，解答企业商业秘密保护专业知识咨询，为企业提供商业秘密保护相关资料。

8.4.2 服务机构可辅导企业建立和完善商业秘密保护工作体系，内容包括但不限于：

——设置商业秘密保护管理组织；

——界定商业秘密保护范围；

——制定和完善商业秘密保护管理制度。

8.4.3 服务机构可指导企业开展商业秘密保护风险与合规排查，并进行风险评估和风险提示。

8.4.4 服务机构可引导并协助企业做好公证、第三方存证、电子存证等证据固定。

8.4.5 企业被侵权时，服务机构可协助维权，包括但不限于：

——协助企业收集证据，整理维权材料；

——引导企业通过合理的途径依法维权；

——协助企业配合行政部门、司法部门等对案件的查处；

——协助做好调解工作。

8.4.6 具备条件的服务机构等可依相应服务资质提供下列专业服务：

——开发、部署和维护涉密文件、数据的信息管理系统；

——提供技术信息的非公知性、同一性和损失数额的鉴定评估；

——提供技术查新、检索委托服务；

——其他专业服务。

附 录 A
（资料性）
商业秘密管理内容及措施

A.1 分级

A.1.1 企业宜对确定的商业秘密进行核查、评估，将商业秘密划分等级，商业秘密的评估可考虑以下因素：

——经济价值，包括现有价值和预期价值；
——投入成本；
——对竞争对手的价值；
——内部可查阅、使用秘密的范围；
——秘密泄露后可能造成的经济损失；
——秘密泄露后可能承担的法律责任；
——其他影响秘密分级的因素。

A.1.2 商业秘密泄漏后有可能影响国家安全和利益的，应依法定程序将其确定为国家秘密。

A.2 清单

A.2.1 企业宜建立商业秘密清单，包括商业秘密名称、主题、密级、保密期限、知悉范围、载体、权属部门、保存方式、存放地点等。

A.2.2 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。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”。

A.2.3 可根据涉密信息的密级以及经营需要，确定知悉范围。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。

A.3 措施

A.3.1 人员管理

A.3.1.1 入职管理

对新入职、转岗到涉密岗位的员工，管理措施包括但不限于：

——与员工签订含有保密条款的劳动合同或专项保密协议，保密条款内容应尽可能详尽、具体；
——与重要岗位涉密人员签订竞业限制协议；
——做好入职前的背景调查，必要时与员工签订不侵犯他人商业秘密的承诺函；
——在录用潜在竞争性关系企业的员工时应：
- 审核待录用的员工与原单位之间的保密约定、保密义务、保密内容及范围，以防范该员工在本企业内部公开或使用原单位的商业秘密；
- 提醒待录用的员工不应将原单位的商业秘密带入本企业进行使用或公开，并要求就本项内容签署不侵犯原单位商业秘密的承诺函；
- 定期对已入职的员工所从事的业务内容进行审核，以排除使用原单位商业秘密。

——做好商业秘密保护教育和培训，在培训结束后宜进行考核，保存相关培训和考核记录。

A.3.1.2 履职管理

对员工的履职管理措施包括但不限于：

——督促员工遵守企业商业秘密保护管理制度，做好本岗位商业秘密保护工作：

- 涉密电子文档、数据、载体、物品等按规定途径和要求使用、流转，并应履行审批和登记手续；
- 按授权使用涉密信息系统及网络；
- 离开工作岗位前及时下线工作账户并设置电脑锁屏。

——对员工进行监督，防止员工未经商业秘密保护部门审批出现下列行为：

- 超范围、超权限或以不正当手段获取使用涉密信息、物品等；
- 拍摄、复制、摘抄、仿造、传播、公开涉密信息；
- 拍摄、测绘、仿造、公开涉密物品；
- 进入非授权涉密区域等。

——定期进行保密教育培训，并保存培训记录。

A.3.1.3 离职管理

对涉密岗位员工转岗、离职的管理措施包括但不限于：

——在员工转岗、离职前主动告知保密义务及违规责任，告知其不应有以下行为：

- 复制、带离、损毁、篡改、拍摄涉密纸质文档、物品；
- 查阅、拷贝、篡改、发送涉密电子文档、数据；
- 删除、更改账户；
- 披露、使用商业秘密等。

——开展离职检查并做好书面记录，检查内容包括：

- 工作电脑数据是否完整，是否有复制、删除痕迹；
- 是否有对外发送商业秘密信息的记录；
- 是否有权限之外的文档、信息数据等；
- 转岗、离职前一定期限内的涉密信息查阅和使用情况等。

——交接所有涉密载体和涉密物品，收回门禁、账号等所有工作权限；

——及时通知与转岗、离职员工有关的供应商、客户、合作单位等，告知工作交接情况；

——向已签订竞业限制协议的员工书面送达竞业限制告知书，告知其保密义务和竞业限制义务，并在法定期限内发放竞业限制补偿金，如不需要员工竞业限制的，及时书面告知并由员工进行确认；

——及时掌握离职员工在竞业限制期限内的任职去向。

A.3.2 载体管理

A.3.2.1 电子载体管理

对电子载体的管理措施包括但不限于：

——涉密非移动电子载体宜禁用移动存储、光驱、蓝牙等数据传输功能，未经权限审批不得随意安装软件；

——涉密移动电子载体宜设置身份识别等加密措施，不可接入非涉密或未采取保密措施的电子设备；

——对涉密电子载体的制作、使用、保存、维修、销毁实施全生命周期管理，履行审批和登记手续，由专人负责并建立台账；

——涉密电子载体不可擅自外送维修，外送维修前宜经商业秘密保护部门审批，并拆卸涉密存储设备或清除涉密信息。

A.3.2.2 纸质文档管理

对涉密纸质文档的管理措施包括但不限于：

——有密级、保护期限等标识，实行登记管理归档存放；

——存放在涉密区域内并由专人管理；

——按权限使用，使用涉密纸质文档履行审批和登记手续；

——废弃涉密纸质文档宜由专人进行销毁，不宜随意丢弃。

A.3.2.3 信息系统管理

对信息系统的管理措施包括但不限于：

——对涉密信息系统实行分层权限管理，以“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；
- 合理分配项目中不同账户的功能和使用期限；
- 合理设定不同账户的访问、操作、查看等权限及其使用期限；
- 合理设定不同账户的互联网使用权限。

——对涉密信息系统采取适当的密码管理方式，如：

- 不使用默认密码，不可设置保存密码自动登录功能；
- 限制设置简单密码；
- 不定期更改密码，最长间隔时间不宜超过三个月；
- 输错密码一定次数锁定账户；
- 同一用户登录不同涉密信息系统宜采用不同密码，确保密码唯一性；
- 设置生物识别进行密码双重验证。

——宜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；

——权限到期、人员转岗、项目或事项变更时及时回收、变更系统权限；

——在涉密信息系统内设置保密义务提醒；

——做好病毒防范、查杀和病毒库的升级等工作；

——定期进行安全检查，发现系统漏洞及时修补；

——定期对涉密信息系统的数据、日志等进行备份并妥善保管；

——信息系统的管理员权限宜在不同员工之间进行分配，避免由超级管理员管理整个系统或若干个系统的情况。

A.3.3 电子数据管理

对涉密电子数据的管理措施包括但不限于：

——存储于企业授权的存储设备和应用系统，不宜存储于非授权存储设备、网络空间；

——对涉密电子数据设置加密措施，加密措施宜与载体有所区别，形成二次加密；

——指定专人进行解密操作，员工按权限使用加密数据；

——收发涉密数据宜使用唯一出入口，对涉密数据流入流出进行审批；

——内部局域网宜与互联网隔离，涉密数据网络传递宜通过内部局域网或加密互联网通道完成；

——通过邮件发送涉密数据时，宜加密和签名，可限定打开次数、打开时限和编辑权限；

——对外发送涉密数据宜经过审批，并采取加密措施，数据发送与密钥发送不宜采用同一通道；

——宜对涉密数据拷贝采取限制措施，拷贝宜履行审批手续并妥善保存拷贝记录；

——涉密电子数据宜做好公证、第三方存证、电子存证等证据固定；
——涉密电子数据销毁时宜确保彻底永久删除，避免可通过其他技术手段进行数据恢复。

A.3.4 物品管理

对涉密物品的管理措施包括但不限于：
——对涉密物品进行标记并单独存放，存放区域按照涉密区域进行管理；
——使用涉密物品宜履行审批和登记手续；
——宜对重要原料、部件等实行编号替代、分部门管理等管理方式；
——对涉密物品的制作、使用、保存、维修、销毁实施全生命周期管理，履行审批和登记手续，由专人负责并建立台账；
——涉密物品需外出携带时宜采取密封、包装等保密措施；
——涉密项目的不良品宜交由专人处理，不可随意丢弃。

A.3.5 区域管理

A.3.5.1 宜列为涉密区域的地点或部门包括但不限于：
——研发设计、信息管理、财务、人力资源等部门；
——实验室、重要生产工作场所；
——控制中心、服务器机房、信息数据中心；
——涉密档案、涉密载体、涉密物品存放地点。

A.3.5.2 对涉密区域的管理措施包括但不限于：
——宜设置物理隔离，形成独立、封闭的区域并设置门禁，张贴明显标识和警示语；
——出入口安装监控和报警装置，采用有效技术手段对出入人员进行身份验证；
——出入涉密区域人员宜履行权限审批和登记手续；
——宜限制使用具有录音、拍照、摄像、信息存储等功能的电子设备；
——必要时采取网络隔离阻断。

A.3.6 商务活动管理

A.3.6.1 隐秘

在商务活动中涉及商业秘密的，宜对相关信息予以隐藏，可采取的隐秘方式有：
——隐藏或删除涉密信息；
——对涉密信息进行模糊化处理；
——其他方式。

A.3.6.2 访问、参观、检查

对访问、参观、检查等活动的管理措施包括但不限于：
——来访人员应履行审批和登记手续；
——宜安排专人陪同访问、参观，限制拍照、录音、录像、信息存储等行为；
——政府部门因检查、监督等工作需要接触涉密信息或涉密物品的，宜提前向其明示保密义务。

A.3.6.3 商务合作

对商务合作活动的管理措施包括但不限于：
——开展商务合作等活动时，宜与相关方或人员签订保密协议约定保密义务；

——聘任可能接触涉密信息或涉密物品的外部人员时，宜签订保密协议，必要时可做背景调查；
——可对合作过程进行控制，对涉密信息或物品的使用情况进行监督管理。

A.3.6.4 涉密会议或其他活动

A.3.6.4.1 涉及商业秘密的会议或其他活动，宜避免使用远程视频、音频或电话会议，可采取下列保密措施：

——选择具有保密条件的场所；
——限定参加人员的范围，指定参与涉密事项的人员；
——告知参加人员保密要求，必要时签订保密承诺书；
——对涉密资料、涉密物品进行控制：
- 确定发放范围，履行发放登记手续；
- 涉密资料、涉密物品有明显的“会后回收”标识提醒；
- 休会或会议结束时，及时收回、清点、登记；
- 保密员可使用专用设备对活动情况通过拍照、录像、签名等方式做好记录。

A.3.6.4.2 涉及商业秘密的远程工作，宜采取下列保密措施：

——经商业秘密保护部门审批；
——对远程网络进行安全鉴别；
——规定硬件和软件的支持与维护要求；
——规定远程工作的环境安全要求；
——授权访问人员，设置访问权限；
——配备专用的操作和存储设备，防止使用私有设备处理或存储信息；
——进行安全监视和过程审核，形成记录；
——远程工作终止时，撤销授权和访问权限；
——企业认为其他有必要的保护措施。

参 考 文 献

[1] 全国人民代表大会 中华人民共和国反不正当竞争法 2019年

[2] 全国人民代表大会 中华人民共和国民事诉讼法 2023年

[3] 最高人民法院 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 法释〔2020〕7号 2020年

[4] 最高人民检察院 公安部 关于修改侵犯商业秘密刑事案件立案追诉标准的决定 高检发〔2020〕15号 2020年