企业商业秘密保护

管理人员工作指引

（试 行）

2025-06-29 发布　　2025-06-29 实施

沈阳市商业秘密保护协会　发布

目　　录

第一章 总则

第 1 条 目的

为提高企业商业秘密保护工作能力，提升企业核心竞争力，指导企业商业秘密管理人员从事商业秘密保护工作，帮助企业有效防范商业秘密泄露风险，提升商业秘密管理水平，保障企业自身商业秘密安全，尊重他人商业秘密，沈阳市商业秘密保护协会在遵循法律理论和总结实务管理经验的基础上，特制定本指引，供有需求企业参考使用。

第 2 条 适用范围

负责企业商业秘密保护管理的工作人员即商业秘密管理人员，在企业商业秘密保护体系建设过程中的工作内容可参考本指引。

具体使用时，还应查询相关最新的法律、法规和司法解释，并充分分析不同企业的差异性需求。

第 3 条 适用效力

本指引为推荐性指引，不具有强制性，各相关企业可在法律、法规、规章有关规定的基础上，参照适用本指引，科研院所、社会团体等其他组织机构的商业秘密保护工作也可参照执行。法律、法规另有规定的，从其规定。

第 4 条 制定依据

1.《中华人民共和国民法典》（中华人民共和国主席令第 45 号）

2.《中华人民共和国反不正当竞争法》（2019 年修正，中华人民共和国主席令第 29 号）

3.《中华人民共和国劳动法》（2018 年修正，中华人民共和国主席令第 24 号）

4.《中华人民共和国劳动合同法》（2012 年修正，中华人民共和国主席令第 73 号）

5.《中华人民共和国刑法》（2023 年修正，中华人民共和国主席令第 18 号）

6.市场监管总局《商业秘密保护规定（征求意见稿）》，征求意见时间为 2025 年 4 月 25 日

7.其它现行与商业秘密相关的法律、法规、部门规章、司法解释及其它规范性文件。

第 5 条 国际条约

1.世界贸易组织《与贸易有关的知识产权协定》

2.《中华人民共和国政府和美利坚合众国政府经济贸易协议》

第二章 商业秘密概述

第 6 条 定义

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。

第 7 条 类型

商业秘密可分为技术信息、经营信息和其他商业信息。

技术信息是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。

经营信息是指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。其中，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。

其他商业信息是指符合商业秘密构成要件，除技术信息、经营信息以外的商业信息。

第 8 条 构成要件

商业秘密保护管理人员在商业秘密保护管理工作中，需围绕商业信息的“秘密性”“价值性”“保密性”开展。

8.1 秘密性

不为所属领域的相关人员普遍知悉，或者不容易获得。

具有下列情形之一的，属于“为公众所知悉”：

1.该信息在所属领域属于一般常识或者行业惯例的；

2.该信息仅涉及产品的尺寸、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.该信息已经在公开出版物或者其他媒体上公开披露的；

4.该信息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。

将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合不为所属领域的相关人员普遍知悉和容易获得的，应当认定该新信息“不为公众所知悉”。

8.2 价值性

能直接或间接为权利人增加收入、降低成本、提高效率或拓展市场的经济利益或者使权利人在市场竞争中处于有利地位的竞争优势。

8.3 保密性

权利人采取与该信息商业价值、独立获取难易程度等相应的、合理的保护措施，这些保护措施在通常情况下足以防止该信息泄露。

第 9 条 常见保密措施

9.1 签订保密协议或者在合同中约定保密义务。

9.2 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。

9.3 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。

9.4 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。

9.5 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。

9.6 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。

9.7 采取其他合理保密措施的。

第 10 条 保护方式

10.1 一项技术或者若干项相关联的技术，可以将部分内容申请专利，部分内容作为商业秘密加以保护。

10.2 技术信息在申请专利前或未公开之前，可作为商业秘密加以保护。

10.3 在满足专利申请需要的前提下，将设备参数等核心技术信息，作为商业秘密加以保护。

10.4 对于技术方案与设计可根据不同情形、不同阶段分别选择先商业秘密后专利加以保护。

10.5 对于容易被以反向工程破解的技术方案或设计，不宜采用商业秘密保护方式，可相应以专利权、著作权等的权利形式加以保护。

第三章 商业秘密保护管理人员岗位认知

第 11 条 岗位定位

商业秘密管理人员是企业商业秘密保护的直接执行者与监督者，负责统筹规划、组织实施保密管理工作，确保企业商业秘密在产生、存储、使用、传递等全生命周期的安全。

第 12 条 核心职责

12.1 制度建设与维护：制定、修订企业商业秘密保护制度、流程及应急预案。

12.2 人员与岗位管理：组织涉及商业秘密管理岗位认定、人员审查、教育培训及考核。

12.3 日常监督检查：开展商业秘密保护检查、风险评估，督促整改泄密隐患。

12.4 应急事件处理：牵头处置泄露商业秘密事件，组织调查、追责与整改。

12.5 沟通协调：协调企业内部各部门及外部监管机构，推进商业秘密保护工作开展。

第 13 条 能力要求

13.1 专业知识：熟悉《中华人民共和国反不正当竞争法》《中华人民共和国刑法》以及最高人民法院、最高人民检察院关于商业秘密司法解释及其他与商业秘密保护相关的法律法规、司法解释及有关政策，掌握商业秘密分类、保护措施等专业知识。

13.2 技能素养：具备风险识别、沟通协调、应急处理能力，熟练使用保密技术工具。

13.3 职业操守：严守保密纪律，具有高度的责任心与忠诚度。

第四章 商业秘密保护管理工作要点

第 14 条 管理机构搭建

14.1 推动领导重视落实

1.明确责任主体：协助企业明确主要负责人为商业秘密保护第一责任人，或推动确定其授权委托人，确保高层对保护工作的直接领导。

2.强化决策支持：定期向管理层汇报商业秘密保护工作进展、风险状况及资源需求，争取将商业秘密保护纳入企业战略规划和年度工作计划，推动高层决策支持制度落地。例如，每季度提交《商业秘密保护工作简报》，包含泄密风险案例分析及资源需求清单。

3.建立监督机制：与高层沟通建立对商业秘密保护管理部门及人员工作的监督考核机制，保障保护制度有效执行。如建议设立专项考核指标，将制度落实情况与部门绩效挂钩。

14.2 商业秘密保护管理部门设置

1.评估企业需求：结合企业规模、行业特点和经营状况，评估是否需要设置专门的商业秘密保护管理部门。若企业规模较小，可建议依托法务、技术管理、人事等部门；若企业规模较大、商业秘密复杂，建议成立独立的商业秘密保护管理部门。可通过开展内部调研，收集各部门对商业秘密保护的需求和建议。

2.确定人员配置：根据部门设置情况，合理规划专（兼）职人员配备。明确人员资质要求，如具备法律知识、熟悉业务流程、有保密意识等，并协助完成人员招聘或内部调配工作。例如，制定《商业秘密保护岗位任职资格标准》，作为人员选拔依据。

3.保障工作条件：为商业秘密保护管理部门争取必要的办公条件和技术设备，如保密文件柜、加密软件、监控系统等，确保工作顺利开展。

14.3 明确商业秘密保护管理部门职责

1.制度建设：制定企业商业秘密保护管理制度，包括总体管理办法、涉密人员管理规定、涉密载体管理办法等配套细则，确保制度覆盖商业秘密全生命周期。

2.事项确定：组织开展商业秘密信息范围界定、密级划分、保密期限设定等工作，明确涉密部门、岗位、人员和区域，制定各生产经营环节的技术防护措施。例如，编制《商业秘密分类分级目录》，明确不同密级信息的保护要求。

3.监督检查：定期组织对业务部门商业秘密保护制度落实情况的监督检查，建立检查标准和流程，对发现的问题及时督促整改，并形成检查报告。

4.教育培训：制定年度商业秘密保护教育培训计划，组织开展法规解读、案例分析、技能培训等活动，提升全员保密意识和能力。

5.事件处理：建立泄密事件应急处理机制，组织对内部泄密事件的调查、处理和整改，协助开展法律维权工作，收集侵权事件证据，配合有关部门进行调查举证。

14.4 促进部门协作联动

1.推动人员配备：协助各业务部门（科技研发、生产经营、人力资源、项目管理等）配备专（兼）职保密员，明确保密员职责和工作要求。

2.建立沟通机制：搭建跨部门沟通平台，定期组织召开保密工作协调会议，交流工作经验，解决协作问题，促进信息共享和协同工作。

3.开展联合工作：与业务部门保密员协作，共同推进商业秘密保护工作，如在项目立项、人员招聘、合同签订等环节，协同落实保密措施。

第 15 条 制度框架搭建

15.1 明确制度搭建原则

1.合规性原则：严格依据《中华人民共和国反不正当竞争法》《中华人民共和国刑法》《中华人民共和国劳动法》等法律法规、部门规章、司法解释，确保制度条款符合法律要求，规避法律风险。

2.适配性原则：紧密结合企业行业特性、经营规模、业务流程等实际情况，使制度具备可操作性和实用性。

3.系统性原则：构建覆盖商业秘密产生、存储、使用、传递、销毁全生命周期的制度体系，确保各环节无缝衔接。

4.动态性原则：定期评估制度有效性，根据企业发展、法规变化及技术更新，及时调整优化制度内容。

15.2 构建制度体系框架

15.2.1 基础管理制度

1.制定《企业商业秘密保护管理制度》，明确商业秘密定义、范围、密级划分标准，确立管理原则、责任主体及总体管理流程，作为制度体系核心纲领。

2.制定《企业涉密人员管理制度》，涵盖涉密岗位认定、人员审查、教育培训、考核奖惩、离岗脱密等全流程管理规范。

15.2.2 专项管理制度

1.在文件与物资管理方面，制定《企业涉密文件资料（物资)管理制度》，规范涉密文件起草、制作、收发、传递、借阅、保存、销毁流程，明确涉密物资采购、使用、保管要求。

2.在设备与系统管理方面，制定《企业涉密设备管理制度》，对涉密计算机、存储设备、办公设备等的采购、登记、使用、维修、报废作出规定，确保设备安全可控；起草《企业信息系统管理制度》，加强涉密信息系统访问权限控制、数据加密、网络安全防护、日志审计等管理，防止信息泄露。

3.在区域与档案管理方面，起草《企业涉密区域（场所)管理制度》，划定涉密区域，明确出入权限、安全防护措施及日常管理要求；起草《企业涉密档案管理制度》，规范涉密档案分类、整理、归档、保管、利用、移交等流程，确保档案安全完整。

15.2.3 业务关联制度

1.在对外活动管理方面，制定《企业对外交流及宣传管理制度》，规定对外合作、商务谈判、学术交流、新闻宣传等活动中的保密审查流程与信息披露规范。

2.在项目合作管理方面，制定《企业研发项目（外部合作）管理制度》，明确研发项目立项、实施、验收及外部合作过程中的商业秘密保护措施，包括合同保密条款约定、信息共享范围界定等。

15.2.4 应急管理制度

制定《企业商业秘密泄露事件处置管理制度》，制定泄密事件分级标准、应急响应流程、调查处理程序、责任追究机制及后期整改措施，提升突发事件应对能力。

15.3 推进制度制定流程

1.需求调研：通过问卷调查、访谈、研讨会等方式，收集企业各部门对商业秘密保护的需求和痛点，分析现有管理漏洞。

2.草案编制：依据调研结果，组织专业人员编写制度草案，明确制度目标、适用范围、管理流程、责任分工及操作标准。

3.意见征集：广泛征求企业管理层、各部门负责人及员工意见，组织内部研讨修订，确保制度符合实际工作需求。

4.审核发布：将制度草案提交企业决策层审核，通过后以正式文件形式发布，并组织全员宣贯培训，确保制度有效落地。

15.4 完善制度维护机制

1.定期检查：每年度对制度执行情况进行全面检查，通过查阅记录、实地检查、员工访谈等方式，评估制度落实效果。

2.动态修订：根据检查结果、企业业务变化、法律法规更新及行业最佳实践，及时修订制度条款，确保制度持续有效。建立制度修订台账，记录修订原因、内容及时间。

3.效果评估：定期开展制度实施效果评估，分析制度对商业秘密保护工作的促进作用及存在问题，为后续优化提供依据。

第 16 条 商业秘密全流程保护步骤

16.1 定密管理

16.1.1 规范流程搭建

1.牵头制定《商业秘密定密管理规范》，明确定密责任人、审核人、承办人职责及权限，建立“提出-审核-审批”标准化流程。

2.组织业务部门、技术团队梳理企业技术信息和经营信息，定期开展商业秘密范围核查与风险评估，形成动态更新机制。

16.1.2 密点确认执行

1.指导业务部门按要求提出拟确定的密点、密级、保密期限及知悉范围，收集研发项目技术交底书、实验原始记录、工艺流程图等商业秘密材料。

2.对提交的定密申请进行审核，重点核查信息涉密属性、密级合理性，审核通过后提交领导审批。

3.监督涉密文件起草即定密、研发成果定期归档、经营信息及时整理归档等工作落实。

16.1.3 信息分类界定

1.依据技术信息（研发、生产、配置等）和经营信息（基础、决策、客户等）分类标准，指导各部门识别商业秘密。

2.建立企业商业秘密分类目录，明确各类信息具体涵盖内容及管理要求。

16.2 分级管控

16.2.1 分级标准实施

1.按企业实际需求，选择三级（核心、重要、普通）或两级（核心、普通）分级体系，明确各密级定义。

2.组织各部门依据经济价值、泄密风险等参考因素，对商业秘密进行分级评估，确保密级划分准确。

16.2.2 层级审批落实

确立分级审批流程，界定不同密级信息的审批权限及流程，监督各部门严格执行审批程序。

16.3 全周期管理

16.3.1 期限与范围设定

1.指导各部门根据信息特性设定保密期限，规范“长期”“公开前”等模糊期限的使用场景。

2.审核知悉范围设定，确保精准限定到具体部门、岗位和人员，监督按密级分类管理执行。

16.3.2 标识与变更管理

1.监督权属部门完成涉密信息载体标识，检查标识内容完整性（名称、编号、密级等）及登记情况。

2.受理密级、保密期限等变更申请，组织审核审批，跟踪权属部门完成标识修改与流程更新。

16.3.3 解密与销毁处置

1.识别解密情形，指导权属部门履行解密申请、审批流程，监督解密措施（移出区域、消除标识等）执行。

2.审核涉密载体销毁清单，现场监督销毁过程，确保符合“视频监控、双人见证、录像存档”要求，规范选择粉碎、物理销毁等合适方式。

16.4 清单化管理

建立企业商业秘密清单，收录名称、密级、接触范围等关键信息，定期更新维护，作为全过程管理核心台账，支撑信息查询、权限分配、流程追溯等工作。

第 17 条 信息系统安全防护建设

17.1 系统建设统筹

1.同步规划设计：在信息系统立项阶段，协同技术部门将商业秘密保护措施纳入建设方案，确保安全防护与系统开发“三同步”（同步规划、设计、建设）。优先选用国产安全保密产品，制定选型标准与采购流程。

2.安全域划分管理：主导划分信息系统安全域，明确各域边界与防护等级。建立跨域数据流转审批机制，部署访问控制设备，严禁高密级信息流向低密级区域，监督安全域与互联网的隔离或加密措施落实。

17.2 安全要求落地

17.2.1 涉密机房安全管控

1.监督机房基础设施建设，确保防火、防水、防雷、防静电、防鼠害、防电磁干扰等安全指标达标，确保涉密基础载体安全。

2.审核机房门禁系统与监控设备部署方案，规范涉密人员出入审批流程，建立外来人员陪同记录台账与管控。

17.2.2 网络安全防护

1.制定网络访问控制策略，部署入侵检测、终端准入等系统，定期开展漏洞扫描与安全评估。

2.建立私联外网、非授权设备接入的监测与阻断机制，留存处置记录。

17.2.3 终端安全管理

1.统一配置终端接入管理系统，实现设备身份识别与访问权限管控。

2.强制涉密终端端口绑定与加密管理，审批外接端口使用申请，监督防病毒软件更新与移动存储介质注册审核。

17.3 用户权限管理

1.身份认证强化：推行多因素认证机制，核心系统强制使用数字证书与口令组合认证。制定口令策略，定期检查账号密码合规性。

2.权限动态调整：按“最小够用”原则分配权限，建立权限变更审批流程。人员岗位变动或项目结束时，48 小时内完成权限回收或重新授权。

17.4 数据安全防护

1.存储加密管理：要求终端与服务器涉密数据全流程加密存储，部署数据完整性监测工具。规范存储介质维修、报废流程，监督专人处理与登记存档。

2.流转安全管控：禁止第三方服务传输涉密信息，审核非内部网络传输加密方案。对外发送涉密信息时，设置阅读权限与有效期，留存操作日志。

17.5 应用安全监督

1.测试应用系统权限设置，确保不影响业务使用前提下实现涉密数据分级管控。

2.强制终端涉密信息显示水印，在系统界面与文件中添加保密提醒标识，定期审计用户操作日志。

第 18 条 涉密信息保护建设

18.1 文件资料全流程管控

18.1.1 标识与登记管理

1.指导部门对涉密文件标注密级、保护期限等标识，建立《涉密文件登记台账》，记录文件名称、密级、存放位置等基础信息，确保登记率 100%。

2.定期对台账更新情况进行抽查，确保新产生的文件能够及时进行登记和归档，以防止遗漏登记。

18.1.2 使用与流转管理

1.规范文件查阅、借阅流程，制定《涉密文件借阅审批表》，明确不同密级文件的审批权限，要求借阅人在台账登记使用时间、接触人员、使用方式、是否复制、是否有泄密风险、归还状态。

2.严格审核文件复制、跨区域转移申请，审批时核查用途合理性与知悉范围合规性，确保复印件等副本与原件同等管理，留存审批记录。

18.1.3 对外发布审核

建立信息发布前审核机制，在新闻、论文、专利等公开内容提交前，由商业秘密保护管理部门对照涉密信息清单，核查是否涉及敏感内容，签署《信息发布保密审核意见表》。

18.2 涉密载体与物品专项管理

18.2.1 存储设备管控

1.监督部门保密员对硬盘、U 盘等存储设备登记造册，标注密级，实行“一人一设备”或“专人专柜”保管，确保存储设备定位可查，建议使用加密存储设备。

2.定期检查存储设备存放环境，确保涉密重点区域物理隔离措施有效，防止未经授权接触。

18.2.2 特殊物品管理

1.针对重要原料、部件，推动采用编号替代、分部门保管方式，切断信息关联泄密风险。

2.严格限制、监控拍摄、测绘、仿造行为，要求相关操作必须提交书面申请，经审批后在专人监督下进行。

18.2.3 流转与维修管理

1.规范涉密载体领用、跨区域转移流程，制定《涉密载体转移审批单》，高密级载体转移需配备双人护送，记录转移时间、路线与交接情况。

2.建立送外维修审批机制，送修前必须拆除涉密存储设备，无法拆除的要求维修方签订保密协议，全程监督维修过程。

第 19 条 涉密场所管理建设

19.1 区域分级与划定

1.科学划定区域：依据涉密信息密级及载体性质，牵头划分涉密、办公、外部接待三级区域，明确产品研发类（产品研发设计、实验室、重要生产场所、数据信息存储中心）、信息管理类（信息管理、财务、人力资源等部门）、涉密档案室类（涉密产品、物品、载体等存放场所）及其他涉密物资类（未公开的样品存放地点；模具、专用夹具、重要零部件存放区；重要原材料、重要半成品等涉密物资存放区等）等部门或场所须列为涉密区域，绘制《企业涉密区域分布图》。

2.动态更新管理：根据变化情况定期组织各部门对涉密区域范围进行复核，结合业务变化调整区域边界及涉密属性，确保划定精准。

19.2 涉密区域基础防护

1.物理隔离建设：监督涉密区域采用实体墙、门禁等物理隔离措施，确保形成独立封闭空间，核查隔断完整性及密闭性。

2.警示标识设置：统一设计并要求在涉密区域入口张贴“涉密区域”“禁止入内”“严禁拍摄传播”等警示标识，确保标识清晰、位置醒目。

3.安防体系搭建：推动企业在涉密区域配置门禁系统、监控设备或安保人员，建立人员出入电子台账，实时监控异常行为。

4.新建改建管控：参与涉密区域新建、改建项目，审核保密防护方案，确保保密措施与工程建设同步，留存验收记录。

19.3 研发区域、生产车间保密管控

1.文件权限管理：制定《研发区域商业秘密文件分级清单》《生产车间商业秘密文件查阅清单》，严格遵循最小权限访问原则，研发人员、生产人员仅能查看与其岗位职责匹配密级的文件，定期抽查文件使用记录，防止越权查阅。

2.台账动态维护：指导研发区域、生产车间建立涉密文件清单及使用台账，要求每周更新文件流转情况，监督清单与文件同步存放于保密柜。

3.复制借出审批：严格审核文件复制、借出申请，核查必要性及知悉范围，留存申请表及领导签字文件，禁止文件违规外流。

4.设备物品管控：禁止手机、拍摄设备进入研发区域、生产现场，设置专人检查手机存放；严禁员工携带涉密设备至研发空间及生产厂房外，违规者依规处理。

19.4 涉密生产设备管理

1.区域专项管理：将涉密设备所在区域纳入重点管控，设置明显保密标识，禁止非涉密人员擅自进入，安装监控设备覆盖关键区域。

2.信息保密要求：监督设备供应商签署保密协议，定期核查协议履行情况。

3.委外作业监督：审核设备委外维修、改造方案，签订保密合同，全程监督作业过程，严禁泄露非必要信息。

4.影像使用审批：严格审批设备拍照申请，限定照片使用范围，对外发布需经保密审查，杜绝信息宣传泄密。

第 20 条 涉密岗位与人员管理

20.1 岗位认定与动态管理

20.1.1 岗位分类核查

20.1.1.1 定期梳理岗位清单

1.每年度联合业务部门更新《涉密岗位目录》，对照技术研发、市场调研、财务数据等涉密场景，逐项确认岗位涉密属性（核心/重要/普通）。

2.重点核查新增岗位或职责调整岗位，如研发项目组新增的测试岗、市场部新设立的竞品分析岗，通过接触涉密信息频率、密级（是否涉及未公开战略）综合判定。

20.1.1.2 差异化权限配置

1.按岗位密级分级授权，核心涉密岗仅开放必要系统访问权限（如研发系统核心算法模块），重要岗限定查阅本部门涉密文件，普通岗禁止接触未公开数据。

2.人员岗位变动时（如从销售岗调至研发岗），24 小时内完成权限回收与新权限审批，同步更新《涉密岗位权限分配表》。

20.1.2 人员准入审查

20.1.2.1 背景调查清单化

1.制定《涉密人员审查》规范，涵盖身份信息（学历、职业资格验证）、信用记录、社会关系（近亲属未在竞品企业任职）、境外活动、与前任单位竞业限制、保密协议等必查内容。

2.核心涉密人员增加心理测评（防泄密风险评估），重要岗位需提供前雇主保密履职证明，审查通过后方可签署《保密承诺书》上岗。

20.1.2.2 分级复审机制

1.一般涉密人员每 2 年复审一次（核查保密考核结果、日常行为合规性），重要岗每年复审（增加职业信用报告核查），核心岗每半年复审（含家庭重大变故影响评估）。

2.复审发现异常（如核心岗员工配偶入职竞品企业、行业异常），48 小时内启动权限冻结，重新评估岗位适配性。

20.2 保密能力提升与考核

20.2.1 分层培训体系

20.2.1.1 定制化课程设计

1.新员工入职：不低于 4 学时保密基础培训，考核通过方可接触基础涉密信息。

2.核心涉密人员：年度不低于 24 学时专项保密培训，邀请行业专家授课，结业需通过攻防演练考核。

3.岗位变动人员：转岗后 1 周内完成新岗位保密要点培训（如从技术岗转市场岗，重点学习客户数据保密规范）。

20.2.1.2 培训效果量化

1.建立《保密培训档案》，记录学员考勤、考核成绩、案例分析表现，作为晋升参考。

2.对考核不合格者，强制参加补考及增加学时强化培训，补考仍不通过者调离涉密岗位。

20.2.2 多维考核评估

20.2.2.1 日常行为积分制

1.制定《涉密人员行为积分表》，设定基础分值，正向加分项、负向扣分项，季度积分低于一定要求启动预警谈话。

2.典型场景：核心岗位员工使用个人 U 盘存储涉密数据，单次扣 20 分并暂停访问权限。

20.2.2.2 年度综合考核

1.从保密意识、制度执行、应急能力三维度评分，考核结果与绩效挂钩。

2.连续 2 年考核优秀的核心涉密人员，优先给予职业发展机会。

20.3 日常监督与风险防控

20.3.1 全场景行为管控

20.3.1.1 涉密载体动态追踪

1.纸质文件：使用编号管理，借阅需填写《涉密文件借阅登记单》，超期未还，管理人员应及时启动商业秘密泄露风险预警机制。

2.电子数据：通过 DLP 数据泄露防护系统监控涉密文件流转，核心数据外发需双人审批，记录操作日志。

20.3.1.2 办公环境合规检查

1.每日抽查涉密场所：门禁系统记录、监控录像、垃圾桶。

2.典型问题处置：如发现员工在会议室未关闭涉密文件即离开、涉密文件未采取保密措施等，当场提醒并记录违规行为，依据保密制度给予相应处理。

20.3.2 全场景行为管控

20.3.2.1 风险预警与处置

1.异常行为监测：建立预警指标库，如涉密岗位员工非正常访问涉密系统、重要岗员工与竞品企业有接触可能，触发系统自动预警，2 小时内启动人工核查。

2.处置流程：经初步核查（调取操作日志、存储证据、询问当事人）后，根据情况进行风险评估（是否涉及泄密），再进行分级处理（口头警告/权限冻结/调离岗位），如已泄密进入应急处理程序。

20.3.2.2 离岗闭环管理

1.离职审批：涉密人员建议提前 6 个月申请，离职前 3 个月启动离任涉密审计（核查涉密文件接触记录），如有意向单位需提供新单位非竞品证明及保密承诺，并进行离职谈话。

2.脱密期管理：按密级设定脱密期（核心岗 1-2 年），在此期间定期提交《个人情况报告》，并接受脱密访谈及必要调查，禁止加入与原职有竞争关系的企业，违反者将依法采取惩治措施。

第 21 条 商业活动管理

21.1 全流程协议管控

21.1.1 协议签订规范

21.1.1.1 必签场景覆盖

1.商务谈判、技术合作、外聘专家、外来参访、外聘律所中介机构、销售等涉及涉密信息的活动，须在活动前与相关方签订《保密合同（协议）》或在主合同中嵌入保密条款，明确保密内容、期限、违约责任。

2.外聘专家、顾问等人员须单独签署《保密承诺书》，明确禁止向第三方披露涉密信息。

21.1.1.2 条款细化要点

1.商业类协议：与商业秘密相关的如确定商业秘密范围、各方保密义务、泄密责任、商业秘密公开程序、商业秘密许可程序、禁止反向工程、转让限制等内容。

2.外来参访协议：限定参观路线、设备使用、资料获取范围。

21.1.2 协议管理流程

21.1.2.1 登记存档

1.建立《商业活动保密协议台账》，记录协议名称、合作方、涉密等级、生效时间及保密期限，核心协议需扫描上传至企业保密管理系统，关联审批流程。

2.外聘人员协议同步录入人力资源管理系统，与考勤、薪酬模块联动，未签署协议者禁止接触涉密信息。

21.1.2.2 资料交付管控

涉密资料交付前，由商业秘密保护管理部门标注密级标识，列明《涉密资料交付清单》并经双方签字确认，纸质文件编号管理，电子文档加密传输。

21.2 专项活动保密要点

21.2.1 技术合作管理

21.2.1.1 过程监督机制

1.委托研发、共同研发项目：设立商业秘密管理档案，指定专人担任保密监督员，根据进度核查合作方涉密信息产生、流转、使用记录，发现异常时立即启动协议违约调查。

2.涉密技术受让项目：在合同中约定“转让方需删除留存的涉密技术资料”，承担保密义务、泄密后承担的责任，并要求对方提供资料销毁证明。

21.2.1.2 成果分配约定

明确技术成果归属：如共同研发约定“双方按出资比例共享商业秘密成果，企业优先使用核心技术”，避免默认条款导致的权利纠纷。

21.2.2 外聘与外来人员管控

21.2.2.1 外聘人员管理

1.使用专用商业秘密保护设备：外聘人员须使用具有防止泄密功能的设备。

2.行为轨迹记录：外聘人员接触涉密信息时，同步开启操作日志审计，离岗前签署《信息清退确认单》。

21.2.2.2 外来参访管理

1.审批流程：参观涉密区域需提前 3 个工作日提交《外来人员涉密区域访问申请表》《参观人员身份信息表》，经商业秘密保护管理部门审核、分管领导审批后，由 2 名以上工作人员全程陪同，对可疑人员做好防泄密措施。

2.安全检查：入场前使用金属探测器检查电子设备，要求参访人员将手机等记录设备寄存至专用保密柜，签署《无涉密设备携带及保密承诺书》。

21.2.3 涉密会议接待

21.2.3.1 场所与人员管控

1.选址要求：选择内部保密会议室，禁用带有网络摄像头的公共会议室，会前检查音视频设备。

2.人员限定：参会人员仅限“必需知悉”范围，名单由商业秘密保护管理部门审核后备案，在会前会后宣布会议为保密会议，如非涉密人员参加涉密会议，需变更为涉密人员并进行管理。

21.2.3.2 文件与设备管理

1.资料管控：涉密会议资料编号发放（如会议纪要标注“2025-05-01 密件”），结束后逐份清点按涉密文件进行处置。

2.设备限制：禁止使用个人设备记录会议内容，确需拍摄的，仅限拍摄非涉密展板，照片需经保密审查后方可导出。

21.3 责任追溯与记录

21.3.1 证据留存

1.往来文件：保存邮件、即时通讯记录、纸质资料签收单、涉密人员违规等证据，核心数据传输需附加《涉密信息传输审批单》作为凭证。

2.外发记录：发送涉密资料时，先审阅接收单位保密义务是否存在，并强调保密义务及泄密责任。

21.3.2 违约处置

发现合作方违规披露涉密信息，立即启动协议违约条款，同时收集证据，必要时发送侵权告知函件。

第 22 条 应急管理

22.1 应急预案体系构建

22.1.1 预案制定与更新

22.1.1.1 标准化预案编制

1.制定《商业秘密泄密应急处理预案》，明确应急组织架构，成立由商业秘密保护管理部门牵头，法务、技术、安保部门参与的应急小组、制定响应流程、责任分工，提前了解商业秘密侵权的主管公安机关、管辖法院、证据保全部门地址及联系方式。

2.结合企业涉密特点细化场景预案，如技术泄密专项预案、合作泄密专项预案，每年度联合法务部、技术部进行实战演练。

22.1.1.2 动态更新机制

依据最新法规及企业发展状态，对企业涉密范围变化包括产生的新密点、已经公开的商业秘密等更新商业秘密管理，定期评估预案适用性，修订后报管理层审批生效并落实执行。

22.2 泄密事件应急处置流程

22.2.1 快速响应与控制

22.2.1.1 线索核实与分级

发现泄密线索如系统异常访问日志、员工举报，应急小组及时完成初步核实，调取操作记录及相关证据、比对涉密清单，按影响程度分级：

1.一级事件（核心商密泄露）：立即启动最高响应，封锁涉事系统、冻结相关账号，保存证据，及时报警。

2.二级事件（重要商密泄露）：及时限制涉事人员权限，隔离涉密区域，保存证据，可选择报警。

3.三级事件（普通商密泄露）：及时完成现场证据保护，启动内部调查，可选择报警与诉讼、行政举报。

22.2.1.2 扩散阻断措施

通过 DLP 数据泄露防护系统追踪涉密数据流向，如外发邮件召回、移动存储设备远程锁定，必要时断开涉事设备网络连接。

22.2.2 调查与损失评估

22.2.2.1 全链条调查取证

1.原因查明：通过监控录像、系统日志、文件移转等线索追溯泄密源头，锁定涉事人员。

2.责任认定：依据《涉密人员行为规范》、《合作协议保密条款》，区分故意泄密过失泄密，形成《泄密事件调查报告》。

22.2.2.2 损失量化评估

由财务部门评估成本损失或委托第三方机构对涉密信息价值、企业经济损失如订单流失、研发成本浪费、声誉影响进行专业评估，评估报告作为维权依据。

22.3 证据收集与固定要点

22.3.1 商业秘密权利人证据链

1.内部文件：提供涉密信息产生记录，如研发项目立项书、会议纪要、定密审批单、证明企业合法持有、保密协议、密点确认文件等。

2.外部文件：侵权人专利申请文件、软件著作权登记证书、与合作方签署的保密协议、侵权人侵权相关证据。

22.3.2 侵权证据收集

22.3.2.1 内容与载体

1.固定商业秘密侵权证据。

2.提取侵权载体形式，包括纸质文件拍照存档、电子数据哈希值固化、数据库操作日志导出，确保不可篡改，建议通过公证云或公证处现场取证。

22.3.2.2 侵权行为证明

1.接触证据：涉事人员权限审批记录、系统登录日志、文件借阅签字单。

2.违规证据：聊天记录，如微信传输涉密文件截图、邮件外发记录、设备检测报告、双方接触照片、侵权人出入侵权单位照片等。

22.3.3 损失与赔偿证据

1.直接损失：客户流失清单、研发投入票据。

2.间接损失：市场份额下降数据、股价波动分析。

第 23 条 多元化维权途径实施

23.1 行政投诉与刑事报案

1.市场监管部门投诉

向市场监管部门提交《商业秘密侵权投诉书》、企业营业执照、涉密信息保密措施说明等材料，并及时跟进处理进度。

2.公安机关报案

针对故意泄密损失较大的，符合《中华人民共和国刑法》第 219 条侵犯商业秘密罪的，向公安机关提交刑事报案材料，并提供商业秘密侵权证据，配合公安部门调查取证。

23.2.民事与仲裁维权

23.2.1 民事诉讼

1.违反竞业限制协议等属于劳动仲裁受案范围的，应先向企业所在地等有管辖权的劳动仲裁委员会申请劳动仲裁，对劳动仲裁结果不服的可以依法提起民事诉讼。

2.不属于劳动仲裁且没有商事仲裁约定的，可向侵权行为地或被告住所地等有管辖权法院起诉。诉讼中，可主张停止侵权、赔偿损失，索赔金额可按实际损失或侵权获利主张，并可向法院提交涉及商业秘密不公开审理申请，要求法院不公开审理；还可申请行为保全，如责令侵权方立即停止使用涉密信息，并进行证据保全等。

23.2.2 仲裁途径

第三方企业或个人违反协议约定的保密义务且约定商事仲裁条款的，应向约定的仲裁委员会申请商事仲裁，仲裁程序非公开、一裁终局，适合涉及商业秘密侵权案件。

23.3 企业内部追责

依据《员工手册》《保密协议》，对过失泄密人员给予降薪、调岗；对故意泄密人员解除劳动合同，追究违约责任，并依据企业商业秘密管理制度给予处罚。

23.4 改进与复盘

23.4.1 漏洞修复

针对泄密原因完善管理措施，如因权限过度开放导致，重新梳理岗位权限；因设备漏洞导致，升级加密系统，及时完成整改并验收。

23.4.2 全员警示

召开泄密事件分析会覆盖全体涉密人员，通报事件经过与处理结果，更新泄密风险案例库，强化员工商业秘密保护意识与应急处置意识。

第五章 附则

第 24 条 解释与修订

本指引由沈阳市商业秘密保护协会负责解释与修订。

第 25 条 特别说明

本指引与法律、行政法规、司法解释等相关法律规定有冲突或不符时，以法律、行政法规、司法解释等相关规定为准。

本指引起草至发布日，国家市场监管总局发布的《商业秘密保护规定（征求意见稿）》正在向社会征求意见，为本指引提供重要参考，若《商业秘密保护规定》正式发布与本指引内容存在冲突，本协会将及时修正指引内容。

针对部分特殊企业既涉及国家秘密，又涉及商业秘密的，可将涉及商业秘密部分定义为“涉商密”，以与涉国密相区分。

第 26 条 实施日期

本指引自 2025 年 6 月 29 日起实施。