

企业商业秘密保护

涉密人员工作指引

(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

前 言	1
第一章 总则	1
第 1 条 目的	1
第 2 条 适用范围	1
第 3 条 适用效力	1
第二章 涉密人员概述	1
第 4 条 涉密人员的定义	1
第三章 通用工作指引	2
第 5 条 涉密人员基本职业道德	2
第 6 条 工作设备与操作安全	3
第 7 条 信息与访问管理	3
第 8 条 物理区域与人员管理	3
第四章 相关岗位涉密人员工作指引	4
第 9 条 高级管理人员	4
第 10 条 研发人员	4
第 11 条 市场与销售人员	5
第 12 条 财务人员	5
第 13 条 采购与供应链人员	6
第 14 条 法务与知识产权人员	6
第 15 条 生产人员	6
第 16 条 支持部门人员	7
第 17 条 实习生等临时人员	7
第五章 附则	7
第 18 条 解释与修订	7
第 19 条 特别说明	8
第 20 条 实施日期	8

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，指导企业实现保护商业秘密目的，规范商业秘密涉密人员管理，防范商业秘密泄露风险，维护企业核心竞争优势，依据《中华人民共和国民法典》《中华人民共和国反不正当竞争法》《中华人民共和国劳动合同法》等法律法规规定，结合企业商业秘密保护实践，制定本指引。

第2条 适用范围

本指引适用于对企业商业秘密负有保密义务的工作人员，即涉密人员。

本指引为涉及商业秘密保密人员在商业秘密保护工作中提供行为参考，具体使用时，应结合岗位特点、办公环境等因素，并充分分析不同企业的差异性需求，灵活把握。

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，结合企业特点，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。

第二章 涉密人员概述

第4条 涉密人员的定义

综合法律法规和部门规章制度，参照《中华人民共和国保守国家秘密法》第四十三条规定并结合各学者的定义，本指引所指的商业秘密涉密人员是指在企业经营管理过程中，因工作需要接触、知悉企业商业秘密、负有保密义务的工作人员，可简称涉密人员。涉密人员通常包括以下几类：

1.高级管理人员：如董事、总经理、副总经理、部门总监等，因其决策和全面管理职责，通常能接触到核心商业秘密。

2.研发人员：工程师、科学家、技术员等，他们是技术秘密如产品配方、工艺流程、源代码、设计图纸的直接创造者和掌握者。

3.市场与销售人员：掌握客户名单、销售渠道、营销策略、投标方案、定价策略等经营秘密。

4.财务人员：掌握成本数据、财务预算、利润信息等涉密财务信息。

- 5.采购与供应链人员：掌握供应商名单、采购渠道、采购价格、物流信息等。
- 6.法务与知识产权人员：直接处理与商业秘密相关的合同、协议、诉讼等。
- 7.生产人员：操作工、班组长等，可能知晓具体的生产工艺流程、设备参数等。
- 8.支持部门人员：可能接触存储商业秘密的服务器的 IT 管理员、文秘档案管理员等，虽然不直接创造或使用秘密，但因工作性质能接触到。
- 9.实习生等：在其工作范围内接触到秘密信息的人员。

第三章 通用工作指引

第 5 条 涉密人员基本职业道德

5.1 忠诚可靠，严守企业秘密

5.1.1 始终维护企业利益，绝不泄露任何涉密信息。

5.1.2 不参与任何可能危害企业商业秘密的活动。

5.2 责任意识强，恪守岗位职责

5.2.1 严格按照保密制度和流程开展工作，确保涉密信息的安全。

5.2.2 主动识别和防范泄密风险，及时报告可疑行为或安全隐患。

5.3 遵纪守法，坚守法律底线

5.3.1 遵守《反不正当竞争法》《中华人民共和国劳动法》等相关法律法规。

5.3.2 不利用职务之便谋取私利，不非法复制、传播或买卖涉密信息。

5.4 诚信自律，杜绝泄密行为

5.4.1 不向无关人员（包括亲友）透露涉密内容，不在私人交往中谈论工作秘密。

5.4.2 在社交媒体、公开场合等谨言慎行，避免无意泄密。

5.5 严谨细致，确保信息安全

5.5.1 妥善保管涉密文件、电子设备及载体，防止丢失或被盗。

5.5.2 使用加密通信工具传输敏感信息，避免通过非安全渠道传递。

5.6 接受监督，配合保密管理

5.6.1 主动参加保密教育培训，提升保密意识和技能。

5.6.2 配合企业商业秘密保护管理部门的检查与审计，如实说明涉密工作情况。

5.7 勇于担当，及时报告隐患

5.7.1 发现泄密事件或潜在风险时，立即向商业秘密保护管理部门报告，并采取补救措施。

5.7.2 不隐瞒、不谎报，积极协助调查处理。

5.8 终身保密，不因时间或岗位变化免责

5.8.1 即使离职或退休，仍需对曾经接触的涉密信息承担保密责任。

第6条 工作设备与操作安全

6.1 禁止使用私人电脑、手机等设备处理工作文件。所有涉密工作必须通过企业配备的加密终端进行操作。

6.2 严禁下载、拷贝、拍照、留存任何工作相关的涉密信息。

6.3 禁止使用公共 AI 等人工智能工具处理、优化或分析涉及企业商业秘密的技术文档或其他涉密信息。

6.4 离开工位时，电脑应当立即关闭或锁定屏幕。

6.5 严禁将个人工作账号、密码外借给他人使用。

6.6 看护好设备，检查保密措施完好性、有效性。

第7条 信息与访问管理

7.1 定期检查并清理个人拥有的系统访问权限清单，及时撤销不再需要的权限。

7.2 涉密配方、核心资料等纸质材料禁止随意放置，严防被拍摄或窥视。使用完毕后必须及时入柜上锁保管。

7.3 报废的硬盘、U 盘、光盘等涉密存储设备，必须按照企业规定由商业秘密保护管理部门集中销毁，不可随意丢弃。

7.4 外部 U 盘、移动硬盘等存储设备，在接入企业系统使用前，必须经过商业秘密保护管理部门指定的安全检测流程检测并确认安全。

7.5 任何形式的涉密信息向企业外部传输，必须提前向商业秘密保护管理部门申请并获得审批。

7.6 对非涉密工作岗位的人员或他人非主观故意透露商业秘密后，及时向商业秘密保护管理部门进行报备。

第8条 物理区域与人员管理

8.1 严格遵守不同涉密区域的进出管理制度。

8.2 保护涉密区域，在涉密区域内发现可疑人员或可疑行为，立即驱离该人员至涉密区域外，并在涉密区域外进行初步询问，了解擅闯原因，并第一时间上报商业秘密保护管理部门。

8.3 发生疑似泄密事件时，全力配合商业秘密保护等管理部门进行调查、固定证据。

8.4 在企业内部陪同非涉密人员时，应时刻注意引导其避开涉密信息区域，不讨论、不展示涉密信息。

8.5 禁止在公共场合处理涉密工作、讨论涉密内容或查阅涉密文件。

8.6 涉密会议结束后，必须立即清理涉密会议内容载体及相关纸质文件，确保无涉密信息遗留。

第四章 相关岗位涉密人员工作指引

第 9 条 高级管理人员

9.1 日常工作中发挥模范作用，带头学习并遵守企业商业秘密保护规则。

9.2 将商业秘密保护工作纳入年度计划与中长期战略，管理并制定商业秘密团队绩效机制，建立商业秘密保护核心人才培养制度。

9.3 及时审查、确认企业员工新发明或发现的商业秘密，符合要求的应及时采取保护措施。

9.4 统筹各部门资源调配，解决跨部门冲突，保障商业秘密保护工作进行顺利。

9.5 监督开展企业商业秘密保护工作，及时听取商业秘密保护管理部门负责人汇报，制定对于已知风险的防范方案。

9.6 代表企业与政府、合作伙伴、协会等商业秘密支持方沟通交流并进行战略合作。

9.7 及时审批商业秘密流程申请，保证流程畅通。

9.8 了解企业商业秘密的直接成本、经济价值，以及泄露商业秘密后对企业的影响。

第 10 条 研发人员

10.1 研发新产品、新技术过程中，及时识别商业秘密并上报商业秘密保护管理部门，在初期及时进行信息同步。

10.2 与知识产权部门、商业秘密保护管理部门合作，对企业核心技术进行分类，确保核心技术得到保护。

10.3 涉及商业秘密的源代码、配方、设计图纸等按企业要求进行分级存储、标记，对使用中的涉密纸质文件妥善保管。

10.4 发布与商业秘密相关性高的学术论文或专利申请前需经商业秘密保护管理部门进行审核，相关性低的应进行脱敏处理，模糊化技术信息、经营信息等数据。

10.5 研发项目涉及商业秘密部分内容分阶段同步内容及授权，采用限定知悉范围原则，保证不同阶段下尽可能减少知情人员。

10.6 指导生产、质检、物流等部门工作时，禁止透露商业秘密。如因工作需要需要对非涉密工作岗位的人员透露，应当向商业秘密保护管理部门进行上报审批。

10.7 项目研发过程中的涉密数据，如实验数据、设计图纸、配方验证结果、算法调优过程按级别进行管理。

10.8 对难以判断的信息本着安全考虑，优先按涉密信息进行管控。

第 11 条 市场与销售人员

11.1 按照企业商业秘密保护制度，将客户信息，包括客户名单、联系方式、需求意向、预算等信息进行保护。

11.2 禁止将客户名单导出至私人设备，必要时可通过企业 CRM 系统进行管理。

11.3 保护涉密信息，禁止私自讨论客户信息、营销策略等涉密信息具体细节，应在商业秘密保护制度下开展工作。

11.4 对外开拓市场、开展营销过程中，均应当注意保守商业秘密。

11.5 对于企业产品销量、产量、成本等影响销售的商业信息严格保密。

11.6 对于有竞争关系的其他企业市场及销售人员进行接触时，妥善保护商业秘密。

第 12 条 财务人员

12.1 严格遵守财务人员的保密职责，对要求保密的信息严格保密。

12.2 使用企业内部财务系统进行工作，禁止将涉密信息下载、拷贝到私人电脑，如利润数据、成本明细等数据。

12.2 禁止通过微信聊天、发送邮件等形式传递涉及企业财务方面的商业秘密信息，发送数据应使用企业加密终端工具。

12.3 涉密数据如财务报表、审计报告等信息外发时，需删除非必要的细节数据，并提交财务负责人及商业秘密保护管理部门负责人双重审核。

12.4 销售量、利润率等涉密重要指标数据出现异常波动的，应立即报告财务负责人，信息出现泄露的，立即报告商业秘密管理部门负责人。

12.5 对外向审计、融资尽调等第三方机构提供数据前，需保护好涉密信息，并审查其保密承诺等文件。

12.6 财务权限在不使用后应当及时申请撤销。

第 13 条 采购与供应链人员

13.1 按照企业商业秘密保护制度，将供应商信息，包括供应商名单、联系方式、产品清单、最低报价等信息进行保护。

13.2 新供应商引入需提前开展背调，符合企业要求的方可引入，签订的合同中应明确保密义务。

13.3 保护涉密信息，保护供应商、价格谈判、成本、采购清单、采购量等涉密信息具体细节，应在商业秘密保护制度下开展工作。

13.4 禁止单独接触供应商，谈判需两人以上在场并记录摘要。对外采购、谈判过程中，均应当注意保守商业秘密，禁止向无关部门透露采购价格。

13.5 禁止将供应商名单导出至私人设备，必要时应通过企业系统进行管理。

13.6 在招标采购过程中，禁止将标底、预算等采购信息提前泄露。

第 14 条 法务与知识产权人员

14.1 所有涉密合同、诉讼材料应当标注密级，存储于加密数字保险柜或带锁实体柜，销毁须经双人复核。

14.2 诉讼中涉及核心商业秘密的，提前向法院申请涉及商业秘密证据的保密处理，关键证据采用分段遮蔽技术提交，并制作非密摘要版本提供法院审理参考。

14.3 按案件、项目设置最小化数据访问权限，禁止跨项目拷贝涉密信息。传输涉密文件应当使用企业加密传输工具，禁止使用个人邮箱、网盘传输。

14.4 所有涉密文档的操作应当使用企业加密工具操作，自动记录操作人、时间及内容片段，日志存档期不少于 10 年。

14.5 与会计师事务所、评估机构、律师事务所、商业秘密保护咨询服务公司等第三方机构合作时，应当签订保密协议并限定保密信息使用范围及泄密后的违约责任等。

14.6 发现泄密风险后立即启动溯源调查，冻结相关账户使用权限并上报商业秘密保护管理部门。

14.7 基于法务人员工作性质，应当及时审查保密措施有效性，并将商业秘密证据按民事诉讼法、刑事诉讼法认可的效力进行管理。

第 15 条 生产人员

15.1 遵守生产区域保密管理制度，经常检查关键工位防窥屏及摄像头完好性。

15.2 禁止携带私人存储、照像设备进入生产区，维修设备需经商业秘密保护管理部门监督执行。

15.3 纸质涉密生产日志、图纸等资料使用应严格保管，经手材料应留痕确认。班组长每日归档至指定保管位置。电子日志修改需按程序授权，修改记录自动同步至商业秘密保护管理部门。

15.4 班组长重点检查异常数据导出及设备使用记录，发现异常立即上报商业秘密保护管理部门。

15.5 生产人员应当仅掌握本单元技术操作细节，涉及保密配方、保密参数等内容时应当通过中央控制系统自动下发，操作界面应当隐藏原始数据且应当设置禁止截屏功能。复杂涉密工艺流程拆分为独立操作单元，核心参数由技术工程师分段授权输入。

15.6 生产人员涉及涉密生产、组装工艺的，在操作时应注意保密，警惕无关人员窥视。

第 16 条 支持部门人员

16.1 服务器实行系统管理、安全审计、日常运维各部分独立运行，数据库涉密字段启用动态脱敏及假名化技术，远程维护需全程录屏操作。

16.2 涉密文件复印、扫描应当使用企业加密终端工具自动叠加含操作者 ID、时间的隐形水印。销毁纸质文件使用交叉碎纸机。访客查阅档案需持动态分级授权码核验通过，应当有相关人员全程陪同且禁止携带电子设备进入。

16.3 对涉密项目按项目周期开通临时权限，项目结束自动收回权限，并对关联存储设备进行格式化验证。权限审批留痕，所有权限申请需经部门负责人与商业秘密保护管理部门双签批。

16.4 对外部人员进行监管，清洁、运维等外包人员进入涉密区域时，IT 部门临时关闭无线网络并部署移动信号干扰器。

第 17 条 实习生等临时人员

17.1 遵守签订的保密承诺书等文件，严格遵守实习单位保密制度。

17.2 对涉密信息按照工作要求隔离处理，替代真实数据操作，处理涉密信息使用分配的虚拟测试环境替代真实数据库。

17.3 指定正式员工作为保密监督人，实习生处理涉密文件的操作需由保密监督人监督并保存。

17.4 禁止进行超权限操作，对已经接触的商业秘密及时上报商业秘密保护管理部门。

17.5 实习结束立即上交门禁卡、账号及纸质笔记，并签署涉密工作交接无留存声明书。

第五章 附则

第 18 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 19 条 特别说明

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“涉商业秘密”，以与涉国密相区分。

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。

第 20 条 实施日期

本指引自 2025 年 6 月 29 日起实施。