

团 体 标 准

T/GZBZ XX—202X

生物医药产业商业秘密保护工作指南

Guidelines for the protection of trade secrets in the biomedical industry

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

202X-XX-XX 发布

202X-XX-XX 实施

广州市标准化协会 发布

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 工作机构 1

5 管理制度 1

6 涉密信息 2

 6.1 涉密信息范围 2

 6.2 涉密信息识别 2

 6.3 涉密信息确定 3

 6.4 涉密信息分级管理 7

 6.5 保密期限和知悉范围 7

 6.6 保密标识 7

 6.7 存管 8

 6.8 流转 8

 6.9 备份 8

 6.10 复制 8

 6.11 发布 8

 6.12 加密与解密 8

 6.13 销毁 8

 6.14 可追溯 8

7 保密管理 9

 7.1 员工管理 9

 7.2 物品与载体管理 10

 7.3 物理区域管理 11

 7.4 外来合作商管理 11

8 监督检查 13

 8.1 检查内容 13

 8.2 检查方法 13

9 评估与改进 13

10 泄密事件管理 13

10.1	内部管理	14
10.2	固定证据	14
10.3	外部维权	14
附录 A（资料性）	保密信息分级指南表	15
附录 B（资料性）	常见载体分类示例	16

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。

本文件由广州市南沙区知识产权发展促进会提出。

本文件由广州市标准化协会归口。

本文件起草单位：广州市南沙区知识产权发展促进会、广东省中绍宣标准化研究院有限公司、广州微斗专利代理有限公司、广东中芯种业科技有限公司、广州源临医疗器械有限公司、广州南沙明曦检测服务有限公司、广州宜生生物医药有限公司、广东金专生物科技有限公司、润尔眼科药物（广州）有限公司、广州非比信息科技有限公司、广州深度医疗器械科技有限公司、广州微远医疗器械有限公司、广州微远基因科技有限公司、广州百康细胞生命科技有限公司、广州同隼医药科技有限公司、广州江元医疗科技有限公司、广州迪澳医疗科技有限公司、广州迪澳基因科技有限公司、广州莲印医疗科技有限公司、广州华银康医疗集团股份有限公司、广州艾基生物技术有限公司、广州埃克森生物科技有限公司。

本文件主要起草人：XXX、XXX、XXX、XXX、XXX、XXX。

引 言

生物医药领域涉及人类生命健康，生物医药产业涉及大量的研发和创新，商业秘密如专利技术、配方、制备工艺等是企业的核心竞争力，保护商业秘密对于维护国家利益和公共安全具有重要意义。近年来，商业秘密纠纷案件呈上升趋势，尤其是在创新能力较高的地区。在司法实践中，权利人举证难、立案难问题突出，商业秘密行政保护方面也存在对侵犯商业秘密的不正当竞争行为规定不够完善等立法和执法与现实需求不适应的情况，企业在商业秘密保护方面仍面临诸多实际问题，需要更具体的指引来规范和加强保护。

本文件的制定旨在为生物医药企业提供具体的商业秘密保护工作指导，帮助企业建立健全商业秘密保护制度，规范保密措施等，提高生物医药企业对商业秘密保护的重视程度，提升企业在商业秘密保护方面的实际操作能力，防范商业秘密被侵犯。

本文件的发布实施将有助于生物医药企业防止技术外泄，保护企业的创新成果，从而维护企业的市场地位，提高企业的经济效益，促进企业创新发展；有利于维护生物医药产业的公平竞争环境，激发企业的创新创造活力，推动整个生物医药产业的健康发展，助力广州市营造良好的营商环境；是对国家法律法规的补充和细化，有助于完善广州市乃至广东省的知识产权保护体系，为生物医药产业的发展提供更有力的保障。

生物医药产业商业秘密保护工作指南

1 范围

本文件提供了生物医药产业商业秘密保护的工作机构、管理制度、涉密信息、保密管理、监督检查、评估与改进及泄密事件管理等方面的建议。

本文件用以指导生物医药产业商业秘密的保护工作。

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

涉密信息 classified information

依照相关法律法规、行业规定或组织内部管理制度，需要采取保密措施进行保护，禁止未经授权泄露、传播或使用的信息。

4 工作机构

4.1 企业最高管理者牵头或在管理层中指定专人作为管理者代表领导商业秘密管理工作。

4.2 依托科技研发、生产经营、人力资源、项目管理等相关部门组建商业秘密管理部门，配备专（兼）职人员，统筹推进制度建设、技术防护、宣传培训与检查评估等工作。

4.3 所有涉及商业秘密的业务部门，配备专（兼）职人员，开展本部门职责范围内商业秘密的保护和管理工作。

5 管理制度

5.1 制定商业秘密保护管理的总体纲领文件，内容可包括商业秘密保护管理的目标、方针、适用范围、定义、策略、原则等，包括但不限于以下管理制度：

- a) 商业秘密信息的识别与分级；
- b) 涉密物品管理；
- c) 涉密载体管理；

- d) 涉密纸质文档管理；
- e) 涉密计算机管理；
- f) 涉密网络管理；
- g) 涉密区域管理；
- h) 涉密人员管理；
- i) 泄密事件管理；
- j) 奖惩管理。

5.2 生物医药企业可根据研发、制造、销售、采购、信息技术、财务、行政等部门的工作流程和特点，分别制定适用于各业务、各部门、各流程的商业秘密保护管理制度，以明确包括但不限于下列商业秘密管理制度的管控对象：

- a) 商业秘密信息及分级；
- b) 涉密人员及岗位；
- c) 涉密计算机；
- d) 涉密物品；
- e) 涉密信息系统。

6 涉密信息

6.1 涉密信息范围

由商业秘密管理部门确定商业信息的收集范围，根据收集范围确定需要开展收集工作的部门，并指定各部门保密员，收集范围包括：

- a) 仅梳理技术信息；
- b) 仅梳理经营信息；
- c) 同时梳理技术信息和经营信息。

6.2 涉密信息识别

6.2.1 企业宜定期/不定期识别研发、生产、经营过程中产生的技术信息和经营信息等商业信息。不定期识别周期参考如下方式确定：技术信息识别周期根据不同研发项目的完结节点确定，其他即时性信息（如市场信息、客户信息等）识别周期以周/月为单位确定。

6.2.2 涉密技术信息包括但不限于：

- a) 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；
- b) 设计图纸、源代码、电路图、数据库结构、器件选型及组合；
- c) 技术路线图、产品路标、生产工艺流程；
- d) 设备仪器的型号、配置参数、特别要求等；
- e) 与业务合作单位协议约定的保密信息。

6.2.3 涉密经营信息包括但不限于：

- a) 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；
- b) 战略发展规划；
- c) 未公开的财务报表；
- d) 上市计划；

- e) 市场调研报告；
- f) 采购渠道和价格。

6.3 涉密信息确定

6.3.1 生物医药

6.3.1.1 新药研发商业秘密确认

生物医药企业宜按照候选分子的发现与筛选、临床前研究、临床试验、新药注册的申请与审批、上市监测与持续研究、知识产权保护、生产、销售的流程确定商业秘密，新药研发流程见图1。

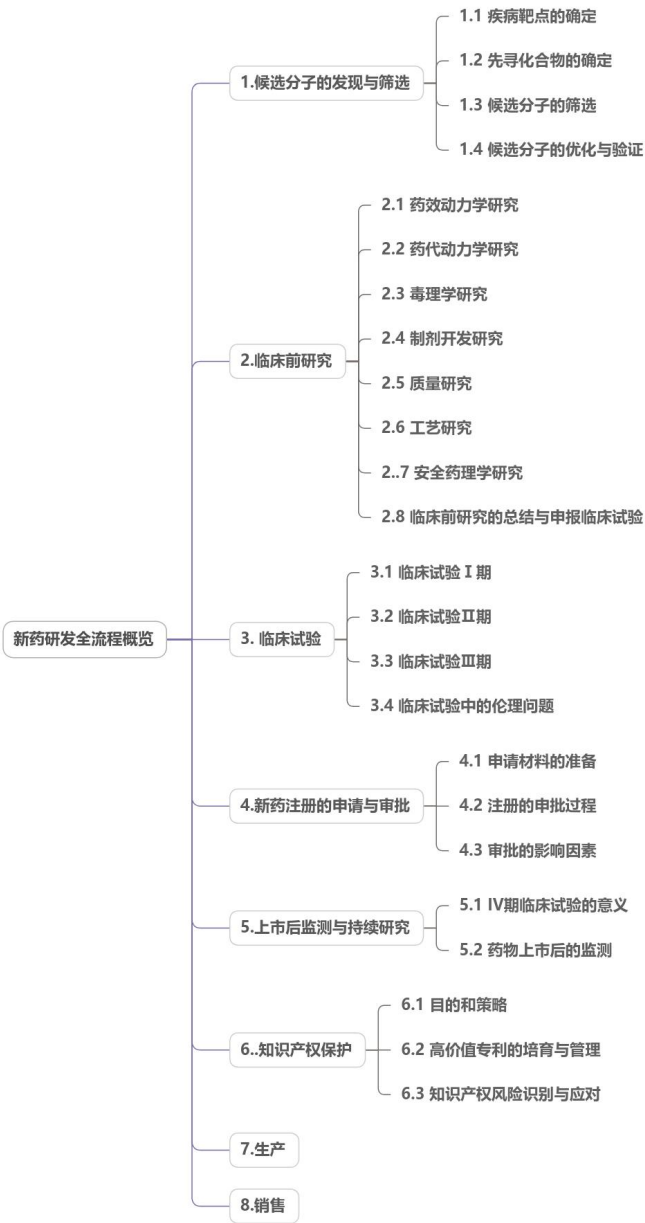


图 1 新药研发流程示意图

6.3.1.2 候选分子的发现与筛选阶段

在候选分子发现与筛选环节，企业宜将药物作用靶点、靶点空间结构、化合物结构、化合物合成路线、检测数据、构效关系数据、适应症、筛选方法、化合物库、检测结果、市场需求等确定为商业秘密。

6.3.1.3 临床前研究阶段

6.3.1.3.1 企业宜按照药效动力学研究环节相关内容确定商业秘密：

- a) 实验设计与模型选择，涵盖独特的动物模型构建（如基因编辑或特定疾病模型）、给药方案的设计与优化（剂量、给药周期、给药途径）、阳性对照药物的选择依据与实验条件优化等；
- b) 数据成果方面包括实验原始数据记录、统计分析方法（如生存曲线拟合算法）、疗效评价指标及其阈值设定（如肿瘤体积变化阈值）等；
- c) 机制研究环节，包括药物作用靶点的发现路径、信号通路解析方法及未公开的靶点结合机制，特别是构效关系分析的技术细节和方法学等。

6.3.1.3.2 企业宜按照药代动力学研究环节相关内容确定商业秘密：

- a) 检测方法与参数包括生物样本处理技术（如超高效液相色谱-质谱联用方法的优化参数）、代谢产物鉴定流程（如同位素标记法及其分析策略）等；
- b) 数据成果包括药物吸收（ C_{max} 、AUC）、分布（Vd）、代谢（CL）、排泄（ $t_{1/2}$ ）等的原始数据及动力学模型参数，尤其是关键代谢酶（如 CYP450 亚型）的抑制或诱导作用数据等；
- c) 特殊场景数据包括药物在特殊生理状态（如肝肾功能损伤）下的代谢特征，或与其他药物联用的药代变化等。

6.3.1.3.3 企业宜按照毒理学研究环节相关内容确定商业秘密：

- a) 实验方案与结果包括动物实验的剂量范围设计、观察指标选择（如神经毒性的行为学检测方法）、病理切片的制备及特殊染色技术等；
- b) 数据成果包括急性/慢性毒性/生殖发育毒性/致癌性等实验的 LD50 /NOAEL 值、各检测指标原始数据及影像学图片、靶器官损伤程度（如肝酶升高阈值）、长期毒性的组织学改变记录等；
- c) 风险评估方法包括基于毒理数据的安全边际计算模型、遗传毒性实验的阴性/阳性判断标准等。

6.3.1.3.4 企业宜按照药物相互作用研究环节相关内容确定商业秘密：

- a) 体外实验数据涵盖酶抑制/诱导实验的底物选择（如 CYP3A4 探针底物）、孵育条件及优化参数（温度、时间、蛋白浓度等）；
- b) 数据成果包括酶抑制/诱导相关参数（如 IC50 值、诱导倍数）、代谢产物生成速率常数及其他关键指标等；
- c) 体内实验设计海内，包括药物联用方案（如与 P-gp 抑制剂的组合）、药代动力学相互作用的预测模型等。

6.3.1.3.5 企业宜按照质量研究环节相关内容确定商业秘密：

- a) 分析方法与标准包括含量测定方法的关键参数（如 HPLC 流动相配比、检测波长选择）、杂质定性定量方法（如手性分离技术）等；
- b) 稳定性数据环节，包括加速/长期稳定性实验的温湿度条件、降解产物的控制限度、包装材料的相容性数据等；
- c) 质量控制策略环节，包括批间差异的统计学控制方法、放行标准的制定逻辑（如依据毒理数据设定杂质限度）等。

6.3.1.3.6 企业宜按照工艺研究环节相关内容确定商业秘密：

- a) 合成路线与反应条件包括创新的合成步骤（如不对称催化反应）、关键中间体的纯化方法、反应温度/压力/催化剂用量的精确控制等；

- b) 放大生产技术包括中试规模的设备参数（如结晶釜的搅拌速率、干燥条件）、溶剂回收与循环利用工艺等；
- c) 制剂开发包括处方组成及各成分占比、制备工艺（如喷雾干燥的进风温度）、包衣材料的特殊配方等。

6.3.1.3.7 企业宜按照药理学研究环节相关内容确定商业秘密：

- a) 实验设计与方案包括核心组合试验的试验设计、模型选择、观察指标、检测方法、观察周期和数据分析算法模型等；
- b) 实验数据与结果包括过程中产生的所有原始数据、综合分析报告等；
- c) 实验材料和流程策略包括特殊实验动物、专用试剂、抗体、传感器、内部管理流程、决策机制和资源分配策略等。

6.3.1.3.8 企业宜按照临床前研究的总结和申报临床试验环节相关内容确定商业秘密：

- a) 技术路线与方法包括研发过程中所采用的独特技术路线、实验方法、工艺流程、特殊的化合物合成方法、制剂制备工艺、实验仪器的独特使用方法等；
- b) 项目计划与规划包括临床前研究项目的总体目标、阶段性目标、时间表、预算安排等；
- c) 申报材料中的关键数据和信息包括临床前研究总结中的实验数据和结果、药物的质量控制信息、稳定性数据、生产工艺信息等；
- d) 与监管机构的沟通内容包括企业在与药品监管机构就临床试验申报进行沟通的过程中，涉及到的对药物研发情况的详细说明、对监管机构问题的答复、以及双方讨论的未公开的意见和建议等；
- e) 临床试验方案包括临床试验的设计思路、受试者的选择标准、给药方案、观察指标和检测方法、数据统计分析计划等。

6.3.1.4 临床试验阶段

临床研究环节，企业宜按照以下工作阶段确定商业秘密：

- a) 临床申请阶段，宜将临床试验中心、药物名称、试验计划、试验目的、临床试验方案、新药名称、药物及活性成分、剂型、制剂处方、给药途径、临床试验目的、适应症、受试者人群、受试者情况（数量、入选及排除标准等）、给药方案、药物安全性评价方法、风险控制计划等确定为商业秘密；
- b) 临床试验阶段，宜将受试者信息、药物信息、试验数据、试验结果、统计分析方法及结果、总结报告等确定为商业秘密。

6.3.1.5 新药注册和审批

新药申请环节，企业宜将药物结构、药物组分、药效毒理及临床等实验数据、临床数据、研究者手册、产品包装、标签设计样稿、制剂处方、生产工艺等注册申报资料确定为商业秘密。

6.3.1.6 上市后监测与持续研究

IV期临床研究（药物上市后监测）环节，企业宜将监测系统、监测数据、评价指标、统计方法、检测结果等确定为商业秘密。

6.3.1.7 新药研发知识产权保护

新药研发过程中产生的知识产权宜及时进行评估和确认，明确保护方式和权益归属，适时形成知识产权：

- a) 不进行专利保护时，宜对其开展商业秘密遴选和分级等工作；

b) 进行专利保护时，在专利申请公开之前，宜采取适当的保密措施保护其技术。

6.3.1.8 生产

生产（含试产）环节，企业宜将生产工艺、工艺参数、生产设备、设备型号、设备参数、关键物料、物料型号/规格、采购需求文件、供应商名录、采购合同、生产计划、质量要求、执行标准、验收标准等确定为商业秘密。

6.3.1.9 销售

销售环节，企业宜将经销商名录、客户信息、代销协议、招投标文件、销售渠道、销售方案、定价机制等确定为商业秘密。

6.3.2 医疗器械

6.3.2.1 医疗器械商业秘密确认

医疗器械企业宜按照立项、研发、型式检测、临床研究、产品注册、生产、销售的制造流程确定商业秘密，相关制造流程如下图 2。



图 2 医疗器械制造流程示意图

6.3.2.2 立项

立项环节，企业宜将市场需求、临床应用场景、性能参数、质量要求、成本评估、市场和技术风险分析、适应症等确定为商业秘密。

6.3.2.3 研发

研发环节，企业宜按照以下工作阶段确定商业秘密：

- a) 系统需求转化阶段，宜将工程技术指标、系统功能架构、设计规范、设计结构、设计指标等确定为商业秘密；
- b) 技术设计阶段，宜将生产工艺、工艺参数、技术要求、测试方法、测试数据、测试结果、产品质量标准、产品图纸等确定为商业秘密；
- c) 测试验证阶段，宜将测试目标、测试数据、测试结果、性能参数、功能参数、测试结果、试验动物、实验数据等确定为商业秘密。

6.3.2.4 型式检测

型式检测环节，企业宜将产品结构、产品原理，主要功能、预期用途、适应症、测试数据等确定为商业秘密。

6.3.2.5 临床研究

临床研究环节，企业宜按照以下工作阶段确定商业秘密：

- a) 临床申请阶段，宜将产品特点、预期用途、临床试验中心、医疗器械名称、试验计划、试验目的、安全性评价方法、有效性评价方法等确定为商业秘密；
- b) 临床试验阶段，宜将受试者信息、筛选标准、产品信息、试验数据、试验结果、统计方法、阶段性临床试验结果、供应商等确定为商业秘密。

6.3.2.6 产品注册

产品注册环节，企业宜将临床数据、产品结构、产品原理、预期用途、检验报告、质量手册、质量记录、产品技术要求、工艺流程、质量管理文件等确定为商业秘密。

6.3.2.7 生产

生产（含试产）环节，企业宜将GMP生产体系中所涉及的生产工艺、工艺参数、生产设备、设备型号、设备参数、关键物料、物料型号/规格、采购需求文件、供应商名录、采购合同、生产计划、质量要求、执行标准、验收标准等确定为商业秘密。

6.3.2.8 销售

销售环节，企业宜将经销商名录、客户信息、代销协议、招投标文件、销售渠道、销售方案、定价机制等确定为商业秘密。

6.4 涉密信息分级管理

6.4.1 分级

企业宜对涉密信息进行分级管理，按层级履行审批手续。涉密信息可分为四级，绝密、机密、内部限制和公开。具体分级描述见附录A。

6.4.2 分级参考因素

企业对商业秘密信息进行定密分级时可考虑以下因素：

- a) 商业秘密信息的经济价值；
- b) 产生商业秘密信息投入的成本；
- c) 商业秘密信息对企业的重要程度；
- d) 竞争对手获取商业秘密后产生的价值；

- e) 商业秘密泄露后产生的经济损失;
- f) 商业秘密泄露后可能承担的法律风险;
- g) 商业秘密信息在企业内部可查阅的范围;
- h) 对商业秘密采取保密措施所需的成本。

6.5 保密期限和知悉范围

6.5.1 保密期限

企业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。一般情况下,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”。

6.5.2 知悉范围

企业可根据涉密信息的密级以及经营需要,确定知悉范围。一般情况下,知悉范围宜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

6.6 保密标识

企业可对涉密信息及其载体实行标识管理,对标识情况进行登记。

- a) 涉密信息标识由涉密信息的名称或编号、密级、保密期限以及权属单位组成;
- b) 涉密信息标识工作由该信息权属部门负责。涉密信息的密级和保密期限等事项一经确定,即在该涉密信息的所有载体上作出明显标识;
- c) 未做标识的涉密信息载体不得进行流转;
- d) 涉密信息的密级、保密期限等事项变更后,权属部门对原标识内容及时进行修改。

6.7 存管

6.7.1 各业务部门宜指定专人负责本部门涉密载体的存档和保管。

6.7.2 宜使用保密柜等具有保密功能的设备来存放涉密载体。常见载体分类命名见附录 B。

6.7.3 存放涉密载体的区域宜配备监控摄像头、火灾报警等安防设备。

6.8 流转

6.8.1 涉密纸质文档的传递可采取密封包装、专人专车、EMS 快递等保密措施。

6.8.2 涉密物品等实物的流转,可采取包装、密封等保密措施。

6.8.3 商业秘密信息只能在企业内部流转,因工作需要流出到外部需要经过审批。

6.9 备份

6.9.1 企业宜定期对商业秘密信息进行备份,可根据商业秘密信息级别的不同分别确定备份保留时间。

6.9.2 企业员工未经审批不能访问备份商业秘密信息,因工作需要临时访问可由负责人进行审批并保留记录。

6.10 复制

6.10.1 企业员工未经授权不得复制或打印商业秘密信息,因工作需要临时复制或打印商业秘密信息可由责任人进行审批并保留记录。

6.10.2 企业员工复制或打印商业秘密信息前宜标明总页数及当前页,打印时必须在打印机旁守候,打印后及时取走不能遗留。

6.11 发布控制

6.11.1 对外发布的内容可能包含商业秘密信息的如论文、网文、产品说明书、用户手册等，发布前宜由商业秘密管理部门进行审批。

6.11.2 涉及商业秘密保护而不宜公开的内容不可申请专利。

6.12 加密与解密

6.12.1 商业秘密信息宜通过企业的加密系统进行加密。加密系统可采取密钥备份、双人控制等安全管理措施。

6.12.2 企业可指定各部门的责任人或保密员管理各部门的解密权限。员工申请解密的，宜明确相应的使用人、项目、具体事由、日期。解密信息宜及时回收并做相应处理。

6.13 销毁

6.13.1 商业秘密信息载体的销毁过程宜采取监督措施，如视频监控、录像、见证。

6.13.2 宜根据商业秘密信息载体的不同采取妥善的销毁方式，确保信息不可恢复。如纸质文档可使用碎纸机彻底粉碎；硬盘、U 盘等宜采用消磁的方式彻底销毁存储内容。

6.14 可追溯

6.14.1 所有商业秘密信息的产生、保存、流转、复制、发布、解密、销毁等均宜保留记录。

6.14.2 记录的留存时间根据商业秘密信息的重要性、储存成本决定。

7 保密管理

7.1 员工管理

7.1.1 入职管理

7.1.1.1 核心技术人员或涉密人员入职前宜调查其工作背景，调查范围包括但不限于：

- a) 过往任职的单位、担任的职务及相关工作内容；
- b) 是否负有保密或竞业限制义务等；
- c) 其他需要调查的内容。

7.1.1.2 企业宜与涉密人员签订竞业限制协议并约定竞业限制的范围、地域、生效条件、期限、违约责任、经济补偿等，竞业限制期限宜限制在 2 年内。

7.1.1.3 涉密人员入职前提醒其需要遵守的保密事项，告知其需要履行的保密义务，并提醒其不可泄露前雇主的保密信息，特别要注意签署员工保密协议。

7.1.1.4 对于涉密人员曾在存在竞争关系的企业工作过的，入职前宜采取脱密措施，包括但不限于：

- a) 涉密人员提供与原企业的保密协议、竞业限制协议等进行尽调；
- b) 提醒涉密人员工作中不能使用原企业的商业秘密信息；
- c) 签署不侵犯原企业商业秘密的承诺函；
- d) 检查确认涉密人员无携带或使用原企业的商业秘密信息。

7.1.2 保密教育

7.1.2.1 企业定期对员工开展商业秘密保密教育并对商业秘密保护知识进行考核。

7.1.2.2 保密培训的形式可以是线下、线上集中培训，或录制成音视频课程：

- a) 对新入职的员工开展保密培训;
- b) 定期对全体员工开展保密培训;
- c) 对重点岗位、重要涉密人员定期开展专项保密培训。

7.1.2.3 企业可通过以下方式对员工开展保密宣传,包括但不限于:

- a) 发放员工手册;
- b) 定期线上向员工推送宣传案例;
- c) 组织答题竞赛;
- d) 在办公场所内张贴宣传标语、播放宣传视频;
- e) 召开全员保密动员大会。

7.1.3 履职管理

7.1.3.1 所在的业务部门宜督促员工熟悉并遵守企业制定的各项商业秘密管理制度,根据以下建议以保护员工所在岗位接触到的商业秘密不被泄露:

- a) 工作中产生的商业秘密信息及时上报商业秘密管理部门登记管理;
- b) 获取、使用、披露企业的商业秘密信息要有授权或取得临时审批;
- c) 获取、使用、披露企业的商业秘密信息要保留相应的记录;
- d) 避免非授权人员获取本岗位的商业秘密信息;
- e) 不进入非授权区域;
- f) 不使用非授权设备、网络、账号。

7.1.3.2 宜建立商业秘密管理奖惩制度,违反企业商业秘密管理规定的处罚结果宜形成书面文件,在企业内部通报并存档,鼓励员工举报违反企业商业秘密管理规定的行为,鼓励员工发现企业商业秘密管理体系、措施、技术授权存在的漏洞,对采纳的线索或意见给予奖励。

7.1.3.3 企业员工参加的工作会议等活动涉及商业秘密的,可采取以下保密措施,包括但不限于:

- a) 在涉密区域内召开;
- b) 使用保密会议室;
- c) 参加会议的员工应具备接触所涉商业秘密的权限或经审批;
- d) 告知其保密要求或签署保密承诺;
- e) 限制使用手机、笔记本或拍摄、录音设备,使用防录音装置;
- f) 重要涉密纸质文档做好标识,会议后检查并回收。

7.1.4 离职管理

7.1.4.1 对涉密离职员工进行离职面谈,告知员工保密义务不因劳动合同的解除、终止而免除。

7.1.4.2 移交所有的原始涉密载体且不得删除或篡改、删除其复制,签收交接清单。

7.1.4.3 回收并注销离职员工所有的 IT 账号或访问权限,及时通知与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。

7.1.4.4 如发现可能侵害商业秘密的,固定证据,按照泄密事件管理规定处理。

7.1.4.5 根据需要决定是否启动竞业限制,定期掌握涉密岗位离职员工在离职后特别是竞业限制期限内的任职情况。

7.2 物品与载体管理

7.2.1 计算机管理,包括但不限于:

- a) 涉密计算机宜使用云桌面系统,数据存储在内部云不宜存储在本地计算机;
- b) 关闭或禁用涉密计算机的移动存储、光驱、蓝牙、无线网卡等数据传输功能模块;

- c) 涉密计算机硬件的配置、维修、报废均需经过审批或授权交由指定人员处理;
 - d) 计算机未经批准不得安装非授权软件;
 - e) 计算机的网络接入、网络配置均需按规定设置,禁止接入非授权网络;
 - f) 涉密便携机宜设置身份验证、硬盘口令,封闭摄像头和麦克风功能,存放时使用带锁的保密柜。不宜在涉密区域使用便携机办公。
- 7.2.2 智能手机或设备管理,包括但不限于:
- a) 涉密区域宜禁止使用个人智能手机或设备;
 - b) 个人智能手机或设备均禁止接入存有商业秘密信息的软件及信息系统如 OA、SAP、CRM 等,避免在个人手机内存储商业秘密信息;
 - c) 个人智能手机或设备禁止接入企业涉密网络。
- 7.2.3 纸质文档管理,包括但不限于:
- a) 涉密纸质文档存放在涉密区域内,打印、复印、扫描、查阅、借用等使用涉密纸质文档由专人专管并登记;
 - b) 企业宜配备打印管控系统管理纸质文档的打印、复印、扫描,并保留记录及备份;
 - c) 废弃的纸质文档通过碎纸机粉碎,不应随意丢弃。
- 7.2.4 产品管理,包括但不限于:
- a) 涉密产品、半成品、原料等的标签需替换为企业内部的编码统一管理;
 - b) 涉密项目的半成品、样品需有专人管理,放置在保密柜或专门的存储室保管;
 - c) 涉密项目的不良品需交由专人处理或报废,不应随意丢弃。
- 7.2.5 移动储存介质管理,包括但不限于:
- a) 未经审批不得使用移动存储设备存储商业秘密信息;
 - b) 涉密存储介质需由专人专管,且使用身份识别、内容加密、设备绑定等保密措施。
- 7.3 物理区域管理
- 7.3.1 办公区域可根据商业秘密信息划分为不同的涉密区域,可按涉密区域、办公区域、外部接待区域三级分区。
- 7.3.2 不同密级的区域之间采取物理门、墙、隔断等物理隔离措施。
- 7.3.3 涉密区域可采取如下保密措施,包括但不限于:
- a) 使用独立、封闭的办公区域,不宜使用开放式办公或多部门混合办公;
 - b) 人员进出需具备相应权限且佩戴明显的身份标识卡,非授权人员因工作需要出入需经审批取得临时授权,外部人员进入需有专人全程陪同;
 - c) 出入口配备安保人员及安防设备;
 - d) 禁止携带手机、笔记本、平板、智能手表等具备拍摄、录音功能的设备器材;
 - e) 禁止非授权人员接入涉密网络;
 - f) 区域内部覆盖实时面部识别、动作识别、异常行为识别的高清摄像头;
 - g) 内部设置专门的涉密会议室或电话室;
 - h) 涉密计算机配备防偷窥、防拍照措施。
- 7.3.4 存放商业秘密信息的数据中心、文档中心宜设置在隐蔽的位置,远离非涉密区域且不宜张贴明确标识以防侵入。
- 7.3.5 涉密区域入口处张贴涉密区域级别标识和禁止携带违禁品标识,区域内部张贴禁止拍摄等禁止标识。
- 7.3.6 涉密区域的出入口可采取以下安保措施,包括但不限于:
- a) 使用指纹、人脸识别、瞳孔等生物识别技术手段的防尾随门禁

- b) 配备检测设备以限制携带手机、笔记本等违禁品出入；
- c) 配备视频监控及报警系统，对非法闯入或携带违禁品进入实时报警；
- d) 设置监控中心并配备专职人员实时监控；
- e) 设置临时储物柜以存放限制物品。

7.3.7 设置专门的外部接待区域用于接待外部人员或用于临时办公、会议，非经审批不允许外部人员进入内部区域或涉密区域办公。

7.4 外部合作商管理

7.4.1 外来人员管理

7.4.1.1 当项目需要外部人员参与时，企业可依据项目的重要程度，选择与对方项目参与人员分别签订保密合同（协议），并组织相关的保密培训。

7.4.1.2 若企业需向行政机关、具有行政管理职能的事业单位等外部单位提供包含商业秘密的资料，必须明确告知对方涉密信息的具体事项以及承担的保密义务。

7.4.1.3 外来参访人员进入公司前需进行登记，并由来访人员签字确认。参访过程中，参访人员需按照指定路线行进，且全程由企业人员陪同。

7.4.1.4 对于需要进入车间、实验室、控制室等涉密区域的参访人员，接待部门需向商业秘密管理部门提出申请并获得审批，同时参访人员要签署保密承诺书。参访人员禁止携带任何拍照、录音录像、存储设备、磁性物质等物品，参观前还需接受安全检查。

7.4.2 技术合作管理

7.4.2.1 在合作研发、委托研发、授权许可、转让出售等技术合作场景中，企业要强化对商业秘密的保密管理。

7.4.2.2 开展技术合作前，企业需对合作方的商业秘密管理能力及侵权风险进行充分调查，同时与合作对象签订技术合作协议等文件。协议中约定以下内容：

- a) 商业秘密的权属，以及使用权限、日常管理和争议处理等方面的内容；
- b) 改进或二次研发产生的“新”商业秘密的权利归属，包括所有权、使用权、转让与许可权、收益权，以及商业秘密成果归员工个人时的优先使用权等，同时明确各方的权利义务；
- c) 其他需要约定的内容。

7.4.2.3 针对不同的合作对象，企业可签订具有针对性的保密协议，明确自身的保密要求、划定保密范围，并与对方商定保密配合措施。

7.4.2.4 技术合作期间，企业要定期监督保密协议的履行情况，一旦发现异常，需及时排查，若确认存在问题，立即采取补救措施。

7.4.2.5 企业在聘任或委托专家、顾问、翻译等专业人员处理商业秘密时，需调查其背景，了解其保密能力、侵权风险以及过往合作企业等情况，避免选择与竞争企业有业务往来的专业人员。

7.4.3 委托生产管理

7.4.3.1 企业在委托生产合作中，要加强对商业秘密的管理，防止在委外生产环节出现商业秘密泄露的情况。

7.4.3.2 当委托生产的部分涉及商业秘密时，企业需评估供应商的保密体系，包括是否制定了完善的保密制度，是否明确了商业秘密的识别、分类、保护、使用和销毁等流程，以及是否定期开展保密义务教育等。

7.4.3.3 对于委托生产的生产区域，企业指派专人负责保密事务，该区域的负责人为保密工作的第一责任人，负责落实相应的管控措施，必要时对第三方人员进行保密培训。

7.4.3.4 开展委托生产合作前，企业要充分考察代工方的生产现场、关键节点控制方法、商业秘密管理能力及潜在的侵权风险。同时，与合作对象签订保密协议，约定商业秘密的使用范围、日常管理责任，确保合作过程中获取的技术信息仅用于委托生产，并明确争议处理方式等内容。

7.4.3.5 在委托生产过程中，若涉及商业秘密信息的传输，需由专人通过加密方式进行；必要时，企业可委派一名或多名代表驻场代工方，协助解决技术问题，以防止商业秘密泄露。

7.4.4 临床试验管理

7.4.4.1 企业要加强临床试验过程中的商业秘密管理，避免在此过程中发生商业秘密泄露事件。

7.4.4.2 企业可全面梳理可能接触到商业秘密的临床试验机构、检验机构等第三方机构名单，并分别与这些机构签订保密协议，约定不同机构的保密内容、保密义务以及违约责任等。

7.4.4.3 企业宜要求第三方机构对存在竞争关系的企业采取信息隔离措施，共同制定信息隔离措施的具体操作流程和办法，并定期进行监督。

7.4.4.4 对于产品（包括样品及配件等）、文件等涉密载体，要进行明确标识；若存在多中心试验、多地送检等情况，还需采取相应的编码措施，对不同的涉密信息载体加以区分。

7.4.4.5 针对临床试验、检验中使用的样品、产品、原材料等涉密载体，企业宜为参与的第三方机构设置回收程序；指派专人负责临床试验、检验产品的档案管理，以及使用、报废记录的登记工作，详细记录试验用生物医药器械、医药试剂的回收、存放、销毁情况，建立档案；临床试验、检验结束后，需依据档案记录进行清点和统一回收；此外，还可设置其他必要的保密程序。

7.4.4.6 对于临床试验过程中产生的医疗数据，企业可根据不同人员的职责设置访问、下载等操作权限，记录相关操作情况，并定期核查操作记录是否存在异常。

7.4.4.7 在关闭临床试验中心工作中，需按流程关闭访视，做好数据清理和数据库锁定工作，确保所有必要文件的完整性，做好财务核算、物资回收、销毁，文档资料归档等工作。

8 监督检查

8.1 检查内容

监督检查内容包括：

- a) 商业秘密保护制度建立与完善情况；
- b) 商业秘密定密、动态管理、存证、保密管理等商业秘密保护与管理工作的开展情况；
- c) 围绕涉密人员、区域、载体及商务活动等不同管理维度的保密措施落实情况；
- d) 其他企业认为有必要检查的内容。

8.2 检查方法

监督检查的方法包括：

- a) 查看涉密纸质文件使用记录；
- b) 查看涉密电子信息载体、信息系统、云存储空间使用记录；
- c) 查看涉密区域的出入口和内部监控；
- d) 现场查验、问询涉密人员工作情况；
- e) 查看涉密商务活动记录及附属合同；
- f) 其他企业认为有必要的监督检查方法。

9 评估与改进

9.1 企业宜配备专门的人员负责商业秘密管理的检查，也可由各业务部门保密员负责各部门的检查工作。

9.2 企业宜采取以下措施并保留记录或原始文件用于检查和评估：

- a) 重要涉密区域的出入口和内部安装监控系统实时监控；
- b) 涉密网络的出、入口实时监控；
- c) 涉密计算机的操作；
- d) 存储商业秘密信息的信息系统；
- e) 对外发送商业秘密信息的软件如电子邮箱、即时通讯软件。

9.3 定期对商业秘密管理情况进行评估并形成报告提交商业秘密管理部门。

9.4 针对定期评估报告发现的管理漏洞制定改进方案、实施计划并执行落地。

10 泄密事件管理

10.1 内部管理

10.1.1 指定内部受理泄密事件报告窗口的负责人，并公开电话、邮箱等联系方式。

10.1.2 制定泄密事件处理流程和应对预案，包括但不限于：

- a) 采取保护措施防止信息进一步扩散或损失扩大；
- b) 调查原因、涉事人员、责任人等；
- c) 收集并固定证据；
- d) 启动内部处罚或外部维权；
- e) 形成报告和改进方案。

10.2 固定证据

企业可采用以下方法固定证据：

- a) 可向专业的商业秘密保护服务机构寻求取证、鉴定、评估等指南和协助；
- b) 发现商业秘密可能被泄露或侵权时，及时收集并固定证据；
- c) 商业秘密信息的非公知性、同一性、损失数额的确定可申请鉴定或评估；
- d) 电子数据类证据申请公证或证据固化。实物和文档类证据要保存原物或原件。

10.3 外部维权

企业可采用以下途径开展商业秘密维权：

- a) 行政查处；
- b) 刑事报案；
- c) 违反竞业限制协议劳动仲裁；
- d) 违反保密协议约定商事仲裁管辖条款的，申请仲裁；
- e) 民事侵权诉讼，或申请诉前禁令。

附 录 A
(资料性)
保密信息分级指南表

保密信息分级描述及范例见表A. 1。

表 A. 1 保密信息分级指南

密级	描述	范例
公司绝密	直接影响公司权益和利益的重要资料，是最重要的公司秘密，泄露会使公司的权益和利益遭受特别严重的损害。	商业绝密：尚未公布的公司发展经营计划，经营策略；对外重大投资计划、投标前方案及重大合同，重要股权变更与会议纪要、重要信函等。 技术绝密：公司专有设计、保密技术方案等重要技术资料。公司开发的专用软件、计算机软件、数据库等。 管理绝密：尚未公开的各种审计报告、财务报表和分析报告、政府关系档案、后勤采购底价和限价、重大人事信息、网络安全资料、重要会议决议和会议纪要、重要信函等。
公司机密	重要的公司资料，泄露会使公司权益和利益遭受到较严重的损害。	商业机密：公司内部掌握的合同、协议或意向书、价格构成明细、成本明细、销售策略与内部会议纪要与业务往来信函等。 技术机密：技术咨询报告、项目文档、研究开发记录、项目数据、技术方案、图纸、技术文档及相关的图片、图表、函电、内部会议纪要等。管理机密：员工人事档案、尚未公布的升降职人事决定及内部会议纪要等。
内部限制	在公司内部需要使用。非授权的披露或破坏不会给公司带来明显危害。	已经公布管理制度、文件和记录、工作流程、员工通讯录、供应商名单和物料供应清单、测试报告、管理流程、客户名单和资料、员工酬、员工考评结果等。
公开	已经对外发布的信息。非授权的披露不会给公司带来影响。	产品广告等公开的推广信息。

附 录 B
（资料性）
常见载体分类示例

常见载体分类示例：

- a) 市场调查、技术调查、预测报告、考察报告、调研综合报告；
 - b) 专利权评价报告、技术论文、技术可行性研究报告、经济可行性研究报告；
 - c) 市场需求分析报告、收益预测分析报告、生产可行性分析；
 - d) 研发方案、实验方案、实验数据、研发可行性分析、研发物料、会议纪要；
 - e) 设备需求、工艺流程、原料采购清单、实验方案、工艺流程、产品规格；
 - f) 临床试验方案、试验数据、数据分析报告、研发配方、设备图纸；
 - g) 工艺流程、设备参数、安装图纸、试研报告、流程改进；
 - h) 设备参数、设备设计图、工艺参数、设备部件、安装图纸；
 - i) 原料配比、中试数据、中试样品、工艺流程、工艺成果、系统代码、软件包文档；
 - j) 检测设备、检测标准、检测结果、数据分析、产品改进方案。
-