成都市生物医疗领域企业商业秘密保护指引

2025 年 11 月

（2025 版）

目录

商业秘密保护指引 1
第一章 总则 2
第一条 制定目的与依据 2
第二条 适用范围 2
第三条 核心定义 2
第四条 基本原则 4
第二章 企业内部保护体系建设 4
第五条 组织架构搭建 4
第六条 商业秘密识别与分级 7
第七条 涉密人员全周期管理 9
第三章 全流程商业秘密防护 14
第八条 研发环节防护 14
第九条 生产环节防护 16
第十条 经营与外部协作防护 19
第十一条 财务与信息系统防护 22
第四章 差异化保护与应急处置 24
第十二条 分规模差异化策略 24
第十三条 应急处置机制 27
第五章 行政、司法与涉外保护 30
第十四条 行政保护流程 30
第十五条 司法保护流程（民事+刑事） 31
第十六条 商业秘密鉴定 33
第十七条 涉外保护 34
第六章 附则 37
第十八条 指引效力 37
第十九条 解释与更新 37
第二十条 附件工具包 38
第二十一条 联系方式 38
附件 1：《商业秘密识别清单表格（参考版）》 39
附件 2：《保密协议（参考版）》 41
附件 3：《竞业限制协议（参考版）》 41
附件 4：《离职保密审计表（参考版）》 53
附件 5：泄密时间应急处置流程（参考图及表） 59
附件 6：其他（参考版） 62

第一章 总则

第一条 制定目的与依据

为护航成都生物医疗产业高质量发展，破解 “高研发投入与低级别保护并存”“跨环节泄密风险突出”“小微企业保护能力薄弱”“跨境泄密应对不足” 等行业痛点，依据《中华人民共和国反不正当竞争法》《四川省反不正当竞争条例》《信息安全管理体系》(ISO27001)、《知识产权强国建设纲要(2021-2035年）》等法律法规及政策文件，结合成都 “中国生物医药产业创新高地” 定位、天府国际生物城等产业集群优势与企业实际需求，制定本指引。

第二条 适用范围

本指引适用于成都市行政区域内从事创新药研发、高端医疗器械制造、数字健康（含医疗 AI 算法开发）、中医药现代化、IVD（体外诊断）试剂研发生产、细胞与基因治疗等生物医疗相关活动的企业、科研机构、医疗机构及专业服务机构，为其商业秘密保护提供 “研发-生产-流通-合作-跨境” 全周期、分场景指导，特别覆盖跨境合作、海外市场拓展中的商业秘密保护需求。

第三条 核心定义

本指引所称商业秘密，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与经营信息，结合成都产业特色及跨境场景补充示例：

技术信息：

创新药领域：一类新药分子结构、Phase I-III 期临床试验原始数据、生物制剂发酵工艺参数；

医疗器械领域：高端影像设备核心算法、可穿戴医疗设备传感器设计方案、骨科植入物材料配方；

中药领域：川产道地药材独家炮制工艺、经典名方二次开发提取工艺、中药复方指纹图谱；

细胞与基因治疗领域：CAR-T 细胞制备流程、基因编辑工具优化方案、干细胞诱导分化技术参数；

生物制造领域：微生物细胞工厂构建基因序列、生物催化反应动力学参数、酶制剂高产菌株筛选工艺；生物基医用材料聚合度调控工艺、发酵罐精准控温参数；

医疗机器人领域：手术机器人运动控制算法、机械臂力反馈传感校准参数；康复机器人患者运动意图识别模型、步态训练轨迹优化程序；

跨境场景：海外注册申报资料、国际合作研发的核心技术转移文档；国际合作生物制造项目的菌株技术许可文件、医疗机器人海外认证测试数据。

经营信息：

市场端：医保谈判报价策略、带量采购投标预案、区域独家代理合作协议条款、海外市场定价策略；

研发端：年度研发管线规划（含未公开靶点信息）、与华西医院等重点医疗机构合作的临床试验方案、国际合作研发的分工与成本分摊协议；

资本端：Pre-IPO 轮融资商业计划书（含未公开财务预测）、并购重组标的评估数据、海外子公司运营数据。

第四条 基本原则

坚持 “政府引导、企业主责、分类施策、协同保护、场景适配、跨境联动” 原则，推动形成 “全周期管理、分层次防护、专业化支撑、区域化协同、国际化应对” 的保护体系，重点强化川产中药、细胞治疗等成都特色领域及跨境场景保护。

第二章 企业内部保护体系建设

第五条 组织架构搭建

（一）大型企业、集团 “三级架构” 岗位职责

层级	岗位、 部门	核心职责	协作要求
决策层	商业秘密保护委员会	1. 审批年度保护预算与工作计划； 2. 审议重大泄密事件处置方案； 3. 决策保护体系重大调整。	每季度召开会议，需研发、法务、财务负责人共同签字确认决议
管理层	商业秘密保护部	1. 制定《商业秘密保护管理制度》及更新； 2. 组织全员保密培训与考核； 3. 监督各部门保密措施执行； 4. 牵头开展泄密事件调查； 5. 统筹商业秘密鉴定相关工作； 6. 对接外部行政、司法及涉外保护机构。	每月与 IT 部门召开技术防护例会，每季度向委员会提交《保护工作报告》
执行层	各部门保密联络员	1. 落实本部门保密措施； 2. 上报本部门泄密隐患及事件； 3. 配合保护部开展培训、审计等工作； 4. 管理本部门涉密载体。	每周向保护部提交《部门保密工作周报》，及时反馈异常情况

（二）中小微企业组织架构简化方案

中型企业：可不设独立保护部门，由法务部牵头，配备 2-3 名专职保密管理人员，承担保护部核心职责，重大事项上报企业管理层决策。

小微企业：指定 1 名高管兼任保密专员，负责签订保密协议、开展基础培训、备份核心数据等关键工作，必要时可外包专业法律服务。

（三）跨部门协作机制

研发部与保护部协作：

新品研发立项时，同步提交《研发项目涉密信息清单》，保护部 1 个工作日内完成分级；

研发数据归档前，需保护部审核存储方式，签字确认后方可归档；

研发过程中涉及外部合作或技术转移时，共同拟定保密条款及信息披露范围。

IT 部与保护部协作：

IT 部每季度对涉密系统开展漏洞扫描，出具《安全检测报告》；

保护部提出技术防护需求，IT 部 5 个工作日内制定实施方案；

共同搭建数据加密、访问控制、日志审计等技术防护体系，定期开展应急演练。

人事部与保护部协作：

新员工入职时，人事部需先获取保护部出具的《岗位涉密等级说明》，再签订对应协议；

员工离职前，人事部需联合保护部开展离职审计，出具《离职保密审计表》后方可办理离职；

涉密岗位招聘时，共同开展背景调查，核实候选人保密相关记录。

法务部与保护部协作：

共同拟定保密协议、竞业限制协议等法律文件；

泄密事件发生后，联合制定维权策略，对接律师及司法机关；

跟踪国内外商业秘密相关法律法规变动，及时调整保护制度。

第六条 商业秘密识别与分级

（一）《商业秘密识别清单（参考）》

信息类别	信息名称	产生环节	载体形式	非公开性判断依据	商业价值评估	保密等级	保密期限	责任人	存储位置	访问权限

信息类别	信息名称	产生环节	载体形式	非公开性判断依据	商业价值评估	保密等级	保密期限	责任人	存储位置	访问权限
技术信息										
经营信息										
技术信息										

（二）分级管控操作细则

核心秘密管控：

生物制造领域 - 工程菌基因序列：电子载体除 AES-256 加密外，额外设置 “基因序列片段拆分存储”；纸质载体存放于“三重防护保密柜”，借阅需生物制造研发负责人、保护部经理、技术总监共同签字批准，且全程在保密室使用，不得带出；

医疗机器人领域 - 反馈校准参数：传输仅限通过企业专属光纤（物理隔离外网），使用 “动态密钥加密”；存储采用 “本地 + 异地双备份”；

核心秘密的鉴定、解密、销毁均需保护委员会审批，全程留存书面记录。

重要秘密管控：

生物制造领域 - 聚合度调控工艺：电子载体采用 “算法 + 访问日志实时审计”；纸质工艺手册使用 “水印防伪”，借阅需生产总监签字，使用后 24 小时内归还；

医疗机器人领域 - 步态优化程序：电子载体除企业 OA 系统权限管控外，额外设置 “代码访问次数限制”；测试报告纸质版存放于带锁文件柜，每月由保护部联合算法部开展一次清点核查；

重要秘密的变更需报保护部备案，解密需保护部审核。

一般秘密管控：

电子载体采用常规加密及权限管理，纸质载体由部门保密联络员统一管理；

定期开展保密检查，确保存储、使用符合基本保密要求；

达到保密期限或失去保护价值的，可按程序解密或销毁。

第七条 涉密人员全周期管理

（一）入职管控细化

背景调查操作步骤：

步骤 1：向候选人发放《涉密岗位背景调查授权书》，明确调查范围；

步骤 2:联系原单位人事管理部门,核实 “是否签订保密 、竞业限制协议”，索取《离职保密确认证明》；

步骤 3：查询中国裁判文书网、企查查，核实候选人是否有泄密相关诉讼或行政处罚记录；

步骤 4：对核心涉密岗位候选人，可委托第三方机构开展深度背景调查，重点核查是否存在侵犯前雇主商业秘密的行为；

步骤 5：形成《涉密人员背景调查报告》，由保护部审核，审核通过方可录用。

协议签署要点：

《保密协议》需明确：涉密信息范围（列举 + 兜底）、保密义务（禁止披露、使用、复制等）、保密期限（含离职后）、违约责任及争议解决方式；

《竞业限制协议》需明确：

竞业限制范围：“成都市行政区域内及海外主要市场（如美国、欧盟）的生物医疗行业，包括但不限于创新药研发、医疗器械制造企业”；

补偿支付：“每月 15 日前通过银行转账支付，补偿标准为离职前 12 个月平均工资的 50%（不低于成都市最低工资标准的 1.5 倍）”；

违约责任：“违反竞业限制义务，需返还全部已获补偿，并支付违约金（金额为补偿总额的 3 倍）”；

注明竞业限制的解除条件及通知方式。

入职培训：新员工入职 1 周内完成保密培训，核心涉密岗位需额外进行专项培训及考核，培训记录及考核结果存档备查。

（二）在岗管理细化

培训考核内容：

基础培训（新员工）：

课程 1:《成都市生物医疗领域商业秘密保护案例解析》(含典型泄密案例及应对)；

课程 2:《保密制度与岗位职责》(结合岗位涉密等级讲解)；

课程 3:《技术防护工具操作》（DLP 系统使用、加密软件操作等）；

考核方式：线上考试（满分 100 分，80 分合格）+ 实操考核；

进阶培训（在岗员工）：

定期开展 1 次 “泄密应急演练”，模拟 “核心数据被拷贝”“员工离职泄密” 等场景，考核员工应急处置能力；

定期开展 1 次法律知识更新培训，涵盖商业秘密民事、行政、刑事保护及涉外保护相关规定；

核心涉密人员每季度开展 1 次保密谈话，记录《涉密人员谈话记录表》，了解思想动态与外部接触情况。

动态监管措施：

建立《涉密人员动态管理台账》，记录姓名、岗位、涉密等级、接触信息清单、培训考核记录、异常行为记录、保密协议签署情况等；

对核心涉密人员的电脑、手机等设备进行必要的安全管控，禁止私自安装未经授权的软件或外接存储设备；

定期核查涉密人员权限，确保仅授予工作所需的最小权限。

（三）离职管理细化

离职审计流程：

步骤 1：离职前 30 天（核心涉密岗位 60 天），人事部向保护部发出《离职人员涉密审计通知》，明确审计时间；

步骤 2：保护部联合 IT 部开展审计：

电子设备：检查电脑、U 盘、移动硬盘，删除涉密数据，出具《电子设备涉密数据清理报告》；

系统权限：取消 OA、数据库、加密服务器等所有系统访问权限，截图留存；

载体回收：收回涉密 U 盘、纸质文件、实验记录本、门禁卡等，填写《涉密载体回收登记表》，需离职人员签字确认；

账号注销：核查并注销离职人员所有工作账号（含邮箱、业务系统等）；

步骤 3：保护部出具《离职保密审计报告》，审计通过方可办理后续离职手续；

步骤 4：向离职人员重申保密义务及竞业限制要求，签署《离职保密承诺书》。

离职后跟踪：

竞业限制期内，每月向离职人员发送《竞业限制履行提醒函》，要求其回复当前工作单位及岗位；

通过行业动态、招聘平台等渠道监测离职人员任职情况，若发现违反竞业限制或泄密行为，立即收集证据，发送《竞业限制违约警告函》，拒不改正的提起诉讼；

核心涉密人员离职后 1 年内，每季度开展 1 次回访，了解其职业动态及保密义务履行情况。

第三章 全流程商业秘密防护

第八条 研发环节防护

（一）实验室防护细化

普通实验室操作规范：

人员出入：每次进入需指纹验证，系统自动记录 “姓名 + 进入时间 + 离开时间”，每月由保护部导出《实验室出入记录表》核查；

实验记录：使用带唯一编号的专用记录本，记录需用不可擦除签字笔，修改处需签字并注明修改时间，禁止涂改或撕页；

废弃物处理：实验废液需倒入专用密封容器，标注 “涉密废液”，由有资质的机构每周上门回收，填写《涉密废弃物回收记录表》，双方签字确认；

禁止无关人员进入实验核心区域，外部访客需经审批并由专人陪同。

特殊实验室防护（如细胞培养室、基因编辑实验室）：

人员管控：进入需 “人脸 + 生物特征（如虹膜）” 双重识别，穿戴专用防护服（印有姓名编号），离开前需经安检（防止携带细胞样本、菌株等）；

操作记录：采用 “电子实验记录系统（ELN）+ 视频监控”双记录，操作过程实时上传至加密服务器，每步操作需研究员电子签名确认，禁止后期修改；

样本管理：样本贴有唯一二维码标签（含样本编号、制备时间、负责人），存储于适宜温度，冰箱需指纹解锁，每次存取记录《样本存取台账》；

实验设备：设置操作权限分级，核心设备（如基因测序仪）的关键参数修改需双人授权，操作日志加密存储且不可删除。

（二）数据防护细化

实验数据区块链存证操作步骤：

步骤 1：研发人员完成实验数据整理后，导出为 PDF 格式，确保数据完整无篡改；

步骤 2：登录常用或相关联的“**知识产权区块链存证平台**”，上传 PDF 文件，填写存证信息（项目名称、数据类型、权属人、联系人等）；

步骤 3：平台生成存证哈希值与存证证书，下载存证证书并打印，与纸质实验报告一并归档；

步骤 4：保护部每季度抽查存证情况，确保 “实验数据生成后 24 小时内完成存证”；

涉及跨境研发的数据，可同步在目标国家认可的存证平台进行存证。

数据分级存储方案：

核心数据（新药靶点、基因序列等）：采用 “离线加密存储 + 异地备份”，存储设备存放于保密柜，访问需多人授权；

重要数据（临床试验中期数据、工艺参数等）：存储于企业内网加密服务器，设置访问权限及操作日志审计；

一般数据（普通实验记录、非核心客户信息等）：可存储于企业 OA 系统，开启基础加密及权限管控。

合作数据共享管控：

与医院、CRO 公司等合作临床试验时，采用 “数据脱敏 + 远程访问” 模式：

数据脱敏：删除患者姓名、身份证号、医院编号等敏感信息，仅保留 “性别、年龄范围、病情指标”；

远程访问：合作方通过企业提供的 “临时访问账号” 访问数据，系统自动记录访问日志，到期自动注销账号；

签订合作保密协议，明确数据使用范围、期限及违约责任，禁止合作方二次披露或用于其他项目。

第九条 生产环节防护

（一）工艺保密

工艺保护：

人员管控：核心工艺操作人员签订《专项保密协议》，约定“离职后不得泄露工艺信息”，企业可为其购买 “保密责任保险”；

工艺记录：采用 “口传心授 + 加密电子记录”，电子记录存储于离线加密硬盘，硬盘存放于双人双锁保密柜；

生产现场：安装 “无死角视频监控”，禁止非授权人员进入，操作人员穿戴无标识工作服，禁止携带手机、相机等拍摄设备；

工艺变更：涉及核心工艺变更时，仅告知必要人员，变更记录加密归档，旧工艺资料按规定销毁。

物料管理：

涉密原料（如附子炮制专用辅料、工程菌菌株）：

采购：与供应商签订《涉密原料供应保密协议》，原料包装标注 “代号”，禁止标注真实名称，明确运输过程中的保密要求；

仓储：存放于独立保密仓库，安装红外报警系统，仓库管理员需指纹 + 密码双重认证方可进入，入库 + 出库需填写《涉密原料仓储台账》，注明 “代号、数量、日期、经办人”；

领用：生产车间领用需出具《涉密原料领用单》，领用后 24 小时内必须使用完毕，剩余原料需当日归还仓库，禁止留存车间；

涉密物料的废弃物处理需符合保密要求，防止信息泄露。

（二）设备保密细化

核心设备（如生物反应器、精密加工设备）管理：

操作权限：设置三级权限（管理员、操作员、维护员），管理员权限仅 IT 部 1 人拥有，操作员仅可操作预设程序，不可修改参数；

使用日志：设备自动记录 “操作人、操作时间、运行参数、故障记录”，日志加密存储，保护部每月导出核查，禁止删除；

设备标识：核心设备标注 “涉密设备” 标识，禁止无关人员触碰或查看。

维修管理：

建议优先选择成都本地有保密资质的服务商；

维修前，企业技术人员拆除设备核心控制系统（含工艺参数的模块），单独保管；

维修过程中，企业人员全程陪同，禁止维修人员拍摄设备内部结构或拷贝数据；

维修后，企业技术人员重新安装核心控制系统，测试正常后方可投入使用，填写《核心设备维修记录表》；

境外设备维修时，需签订保密协议，明确禁止技术信息泄露，必要时由企业技术人员全程监督。

第十条 经营与外部协作防护

（一）医保谈判报价策略保护

策略制定阶段：

参与人员：在 “保密会议室” 内讨论，讨论资料为纸质版，使用后立即粉碎；

报价文件：采用 “分层加密”，外层为企业 OA 系统加密，内层为 PDF 密码加密，仅在谈判前由专人送达谈判现场；

限制参与人数，明确每个人的信息知悉范围，签订《谈判保密承诺书》。

谈判实施阶段：

现场人员：授权代表携带加密笔记本电脑（无外接接口）参会，电脑内仅存储报价文件，谈判结束后立即删除；

信息反馈：授权代表每日通过加密电话向公司汇报谈判进展，禁止使用微信、短信等普通方式；

谈判结束后，回收所有相关文件，统一销毁或加密归档。

（二）客户信息保护

客户信息分级：

核心客户（如长期合作的大型医院、独家代理商）信息：按核心秘密管控，存储于加密服务器，仅销售总监及指定客户经理可访问；

重要客户信息：按重要秘密管控，设置访问权限，禁止私自拷贝或披露；

普通客户信息：按一般秘密管控，规范存储及使用流程。

客户信息使用规范：

禁止销售人员私自记录客户敏感信息（如负责人私人联系方式、特殊合作需求）；

客户信息通过企业统一的 CRM 系统管理，离职人员无法带走客户数据；

与客户签订合作协议时，明确双方保密义务，保护客户商业秘密的同时，也要求客户保护企业相关信息。

（三）外部合作方管控（CRO、CDMO、供应商等）

筛选阶段：

资质审查：除常规资质外，需审查 “商业秘密保护体系”，要求提供《保密管理制度》《近 3 年无泄密记录证明》；

实地考察：前往合作方办公地点，检查其数据存储环境、人员管理（如是否签订保密协议）、物理防护措施等；

背景调查：通过行业口碑、裁判文书网等渠道，核实合作方是否存在泄密历史或相关纠纷。

合作阶段：

协议条款：明确 “数据使用范围仅限本项目、不得用于其他研究；未经甲方书面同意，不得分包给第三方；项目结束后 7 天内归还所有涉密资料并删除电子数据，出具《数据删除确认函》；涉及跨境合作的，明确适用法律及争议解决方式”；

过程监管：

每月要求合作方提交《保密工作执行报告》，说明数据使用、存储情况；

每季度开展 1 次现场检查，查看数据存储日志、人员培训记录，抽查员工保密协议签署情况；

对合作过程中涉及的涉密信息披露，实行 “按需披露、分级披露” 原则，避免过度披露核心秘密。

项目结束：

回收所有纸质资料，IT 人员远程核查其服务器，确认数据已删除，双方签署《项目保密终止确认书》；

对合作过程中产生的涉密载体（如硬盘、U 盘、实验样本）进行回收或销毁。

第十一条 财务与信息系统防护

（一）财务信息保密

涉密财务信息范围：研发投入明细、盈利预测数据、医保谈判成本核算、并购重组财务数据、涉外合作财务条款等。

保密措施：

不得在不利于保密的场合谈论涉密财务信息，不得在未经批准的情况下随身携带涉密财务资料；

与财务相关的重要文件、软件、报告应设置密钥，指定专人保管，密钥密码定期更换；

查阅重大交易记录、重要财务数据需提出申请并逐级审批，经商业秘密管理人员最终审批通过后，方可调阅；

网银业务系统由专人管理，管理人员需经严格资信调查，定期检查系统保密性。

（二）信息系统全面防护

网络安全：

构建 “防火墙 + 入侵检测系统 + VPN” 的网络防护体系，防止外部攻击和未经授权的访问；

涉密网络与互联网物理隔离，核心数据禁止接入外网；

定期更新系统及软件补丁，关闭不必要的端口和服务。

数据加密：

对敏感数据（如研发数据、临床试验结果、客户信息）进行加密存储和传输，采用 AES-256 等高强度加密算法；

电子文档、邮件等设置访问密码和操作权限，禁止私自转发或拷贝。

访问控制与日志审计：

实施严格的用户权限管理，遵循 “最小授权” 原则，确保员工只能访问与其工作直接相关的数据和系统；

对系统操作进行详细记录，包括登录、查询、下载、修改等行为，日志至少保存 1 年，保护部每月进行审计，及时发现异常行为；

对核心数据的访问实行 “双人授权”，重要操作需二次验证。

备份与恢复：

定期对重要数据（研发数据库、临床试验数据、财务数据等）进行备份，核心数据采用 “本地 + 异地 + 云端” 三重备份；

制定数据恢复预案，每半年开展 1 次备份恢复测试，确保数据安全；

备份介质加密存储，由专人管理，明确备份周期（核心数据实时备份，重要数据每日备份，一般数据每周备份）。

移动设备管理：

实施移动设备管理策略，控制公司数据在移动设备上的存储和访问，禁止私自使用个人移动设备存储涉密数据；

必要时可远程擦除移动设备中的公司数据，设置设备锁屏密码及自动锁屏时间。

第四章 差异化保护与应急处置

第十二条 分规模差异化策略

（一）大型企业

高级防护措施：

跨境保护：设立 “海外商业秘密保护专项小组”，配备熟悉国际规则（欧盟《商业秘密指令》、美国《Defend Trade Secrets Act》）的法务人员；

协议管理：与海外合作方签订双语《保密协议》，明确适用法律**（优先选择中国法或双方认可的第三国法）**及争议解决方式（仲裁机构选择中国国际经济贸易仲裁委员会等）；

建立 “数据分类分级体系 + 数字水印 + 数据防泄密系统”的全方位技术防护；

定期开展商业秘密审计，委托第三方机构评估保护体系有效性。

成都本地资源对接：

国际合作：对接欧盟知识产权局（EUIPO）、美国专利商标局（USPTO）资源，获取海外商业秘密保护指引；

风险预警：实时获取目标市场商业秘密侵权案例及法规变动信息；积极共享保护经验及资源。

（二）中型企业（聚焦重点防护）

核心措施：

建立信息安全管理体系，可申请 ISO27001 认证或网络安全等级保护测评；

对关键岗位人员开展背景调查，核心技术人员签订竞业限制协议；

采用 “网络隔离 + 统一账号管理 + 双因子鉴别” 的技术防护方案；

重点管控研发、生产环节的核心秘密，简化一般秘密管理流程。

资源利用：

依托生物医药集中园区，获取咨询、存证等一站式服务；

与本地律师事务所合作，建立常态化法律服务机制，降低维权成本。

（三）小微企业关键措施：

核心思路：以 “可用性” 为核心，确保核心商业秘密不丢失、不泄露；

协议签订：与所有员工签订保密协议，核心技术人员补充签订竞业限制协议；

数据备份：对关键性数据进行实时备份，其他数据每日备份，使用知名云服务提供商的产品；

安全基础：确保办公计算机杀毒软件有效启用并更新，员工账号一人一号，启用登录日志；

人员培训：将安全意识培训纳入入职及周期性考核，重点强调核心数据保护要求。

风险规避：

避免核心秘密集中在单一人员手中，关键信息至少两人知晓；

对外合作时，谨慎披露信息，优先选择有保密资质的本地合作方；

定期检查保密协议签署、数据备份等关键措施落实情况。

第十三条 应急处置机制

（一）泄密事件分级标准（参考）

泄密等级	判定标准	示例
一级（特别重大）	核心秘密泄露，预计损失超 5000 万元；或引发国际纠纷；或导致研发项目停滞 6 个月以上	一类新药分子结构泄露，竞争对手提前申报专利；CAR-T 制备工艺泄露，海外企业仿造
二级（重大）	核心秘密泄露，预计损失 1000-5000 万元；或重要秘密泄露，预计损失超 500 万元；或导致市场份额下降 10%以上	医疗器械核心算法泄露，竞争对手产品提前上市；医保谈判报价策略泄露，影响中标结果
三级（较大）	重要秘密泄露，预计损失 100-500 万元；或一般秘密泄露，预计损失超 100 万元；或导致业务开展受阻	生产工艺参数泄露，引发同行低价竞争；重要客户名单泄露，核心客户流失

泄密等级	判定标准	示例
四级（一般）	一般秘密泄露，预计损失 10-100 万元	普通供应商信息泄露，影响采购议价；非核心实验数据泄露，无重大业务影响

（二）应急响应流程（分等级处置）

一级泄密（2 小时内启动）：

立即处置：

封锁信息源：断开涉事设备网络连接，冻结相关数据库访问权限，回收所有涉密载体；

固定证据：由 IT 部门提取操作日志、邮件记录，委托公证处进行证据保全，同步通过区块链存证；

内部通报：仅向 “商业秘密保护委员会” 成员通报，禁止扩散信息，避免引发股价波动或合作方恐慌；

48 小时内行动：

成立专项小组：由法定代表人牵头，联合法务、研发、外部律师组成，制定处置方案；

外部联动：向成都市市场监督管理局提交《重大商业秘密侵权投诉书》，同时对接市知识产权保护中心，申请 “行政保护 + 司法保护” 联动；

跨境应对：若涉及海外泄露，通过 “成都国际知识产权运营中心” 联系当地知识产权保护机构（如欧盟 IPOSS），启动海外维权协助；

损失控制：评估泄露影响，调整研发方向、变更核心技术参数或市场策略，降低损失扩大。

二级泄密（24 小时内启动）：

立即处置：

限制信息传播：通知相关部门停止使用涉事信息，撤回已发送的涉密文件；

证据固定：由保密管理员联合 IT 部门提取证据，通过区块链存证；

初步调查：核实泄密范围、途径及责任人；

72 小时内行动：

内部调查：由保密管理部牵头，3 个工作日内出具《泄密事件调查报告》，明确责任人；

外部投诉：向市监局提交投诉材料，申请行政查处；

损失控制：调整受影响业务（变更研发靶点、修改报价策略等），降低损失扩大；

整改措施：针对泄密漏洞，1 周内完成整改，加强相关环节防护。

三级 + 四级泄密（24 小时内启动）：

处置步骤：

证据固定：由保密联络员提取相关记录，登记《泄密事件台账》；

内部处理：对责任人进行约谈（三级泄密）或警告（四级泄密），调整涉密岗位权限；

风险整改：针对泄露漏洞，1 周内完成整改；

损失评估：核算实际损失，必要时要求责任人承担相应赔偿责任。

第五章 行政、司法与涉外保护

第十四条 行政保护流程

（一）投诉举报渠道

实名注册并登录全国 12315 平台（网址：www.12315.cn）进行举报；

拨打成都市场监管部门投诉举报热线 028-12315 或市民热线 028-12345 进行举报；

向辖区内市场监管部门现场提交举报材料。

（二）举报材料准备

商业秘密的具体内容（明确密点）、载体及证明其不为公众所知悉的材料；

已采取的保密措施说明（如保密协议、制度文件、技术防护记录等）；

被侵权事实证明（如侵权人获取、使用、披露商业秘密的证据）；

权利人主体资格证明（如营业执照、法人身份证明等）；

其他相关材料（如损失评估报告、合作协议等）。

（三）行政查处配合

配合市场监管部门开展现场检查、调查取证等工作，提供相关证据材料；

如需进行商业秘密鉴定，配合选定鉴定机构，提交鉴定所需资料；

对行政查处结果有异议的，可依法申请行政复议或提起行政诉讼。

第十五条 司法保护流程（民事+刑事）

（一）民事诉讼要点

管辖法院：

技术秘密民事纠纷案件：由成都知识产权法院管辖；

经营秘密民事纠纷案件：由侵权行为地或被告住所地的基层人民法院管辖。

诉讼准备：

明确密点：在一审法庭辩论终结前明确商业秘密的具体内容，剔除公有领域信息；

证据准备：收集权利证据（研发记录、权属证明等）、保密措施证据、侵权证据（侵权产品、交易记录等）、损失证据（审计报告、评估报告等）；

申请保全：必要时申请证据保全或行为保全，防止证据灭失或损失扩大；

诉讼策略：根据案件情况申请不公开审理，避免诉讼过程中进一步泄密。

（二）刑事保护适用

追诉标准：

给商业秘密权利人造成损失数额或违法所得数额在 30 万元以上的，构成 “情节严重”；

损失数额或违法所得数额在 250 万元以上的，构成 “情节特别严重”。

报案流程：

向公安机关提交报案材料（含商业秘密证明、侵权事实证明、损失评估报告等）；

配合公安机关开展侦查工作，如需鉴定，由办案机关委托有资质的鉴定机构。

（三）刑民交织处理

对于侵犯经营信息类案件，可采用 “先民后刑” 模式，先通过民事诉讼查明权利归属及侵权事实；

对于侵犯技术类案件，较易达到刑事追诉标准的，可采用 “先刑后民” 模式，借助刑事侦查手段固定证据；

积极配合司法机关工作，合理选择维权路径，最大化保护自身权益。

第十六条 商业秘密鉴定

（一）鉴定种类及适用场景

非公知性鉴定：判断涉案信息是否不为公众所知悉，是商业秘密认定的基础；

同一性鉴定：对比侵权信息与权利人商业秘密是否相同或实质相同，是侵权认定的关键；

损失鉴定：评估商业秘密被侵权造成的损失或侵权人违法所得，用于确定赔偿数额。

（二）鉴定机构选择

可通过人民法院诉讼资产网（https://www.rmfysszc.gov.cn）查询选择有资质的知识产权鉴定机构；

优先选择具有生物医疗领域专业背景的鉴定机构，确保鉴定结果的科学性和准确性；

成都市及周边推荐鉴定机构清单（可通过市知识产权保护中心获取）。

（三）鉴定注意事项

密点选取：合理梳理密点，避免过多或过少，确保密点具有针对性和可比对性；

材料提交：提供完整、真实的鉴定材料（如技术文档、样品、实验数据），配合鉴定机构开展工作；

鉴定意见质证：鉴定意见需经庭审质证，对鉴定结论有异议的，可申请鉴定人出庭或申请重新鉴定。

第十七条 涉外保护

（一）主要国家 、 地区保护规则摘要

美国：

立法：《统一商业秘密法》《经济间谍法》《保护商业秘密法》构成三重保护体系；

救济途径：民事诉讼（可主张禁令、损害赔偿及惩罚性赔偿）、刑事程序、337 调查（快速排除侵权产品进入美国市场）；

注意事项：美国实行 “长臂管辖”，即使侵权行为部分发生在美国境外，也可能被管辖。

欧盟：

立法：《商业秘密指令》统一欧盟各国保护标准，要求成员国制定相应国内法；

救济途径：申请临时禁令、损害赔偿（可选择利润损失、许可费或侵权人获利作为计算依据）；

注意事项：注重数据跨境传输中的保密保护，需符合 GDPR 相关要求。

日本：

立法：主要通过《不正当竞争防止法》规制侵犯商业秘密行为；

救济途径：民事禁令、损害赔偿，刑事制裁最高可处 10 年监禁及 3000 万日元罚金；

注意事项：检察官可独立提起诉讼，但需权利人配合提供证据。

（二）中国企业涉外应对策略

事前预防：

了解目标市场保护规则：提前学习当地商业秘密定义、保密措施要求及维权途径；

完善内部跨境管控：建立跨境信息传输审批制度，加密传输核心数据，避免核心秘密集中存储于海外；

审慎招聘：招聘海外员工或有海外工作经历的员工时，开展背景调查，明确其不得携带前雇主商业秘密；

协议防护：与海外合作方签订双语保密协议，明确适用法律、争议解决方式及保密义务。

事中应对：

证据固定：一旦发现泄密，立即固定侵权证据（如邮件、交易记录、产品样本），通过当地公证或存证平台保全；

聘请专业律师：选择熟悉当地法律及生物医疗领域的律师，制定维权策略；

联动国内资源：通过成都国际知识产权运营中心、商务部等机构，获取海外维权支持。

事后救济：

选择合适救济途径：根据案件情况选择民事诉讼、刑事报案或行政投诉，美国市场可考虑 337 调查；

损失追偿：积极主张损害赔偿，包括直接损失、间接损失及合理维权开支，恶意侵权可主张惩罚性赔偿；

风险规避：总结经验教训，优化海外保护体系，避免再次发生泄密。

第六章 附则

第十八条 指引效力

本指引为指导性文件，不具有法律约束力，企业可结合自身实际调整实施；涉及具体法律问题，建议咨询成都市知识产权保护中心或专业律师。

第十九条 解释与更新

本指引由成都市市场监督管理局、成都市知识产权保护中心负责解释，根据《中华人民共和国反不正当竞争法》修订、生物医疗产业发展及企业需求变化，每 2 年更新 1 次。

第二十条 附件工具包

包含《商业秘密识别清单表格（**参考版**）》《保密协议模板（**参考版**）》《竞业限制协议模板（**参考版**）》《离职保密审计表（**参考版**）》《泄密事件应急处置流程图（**参考图**）》等实用文件，可通过“成都市知识产权公共服务平台”下载。

第二十一条 联系方式

成都市市场监督管理局反不正当竞争处：028-85394673

成都市知识产权保护中心：028-89139916

附件 1：《商业秘密识别清单表格（参考版）》

商业秘密识别清单表格

（参考版）

企业名称：_____

清单版本：

更新日期：_____年____月____日

责任部门：商业秘密保护部、保密专员

适用范围：研发、生产、经营、外部合作等全环节涉密信息

序号	信息类别	信息名称	产生环节	载体形式	非公开性判断依据	商业价值评估	保密等级	保密期限	责任人	存储位置及方式	访问权限范围	备注

填写说明

信息名称：应具体明确，避免笼统表述；

载体形式：根据实际存储方式勾选，可补充其他载体；

非公开性判断依据：应附具体证明材料，标注编号便于追溯；

商业价值评估：结合信息对企业盈利、竞争优势的影响程度判定；

保密等级：核心秘密（影响企业生存发展）、重要秘密（影响业务开展）、一般秘密（轻微影响）；

存储位置及方式：需明确具体存储地点、加密方式、防护措施（如“加密服务器 + 双人双锁”）；

访问权限范围：明确具体人员姓名或岗位，遵循 “最小授权”原则；

备注：关联相关项目、协议、客户等信息，便于后续管理。

配套使用工具

证明材料台账：单独建立《涉密信息证明材料清单》，对应本表“非公开性判断依据” 编号归档；

载体管理台账：针对电子载体（U 盘、硬盘）、纸质载体（合同、手册）建立单独管理台账，记录领用、归还、销毁情况；

权限变更记录：若访问权限发生调整，填写《商业秘密访问权限变更申请表》，经责任人审批后存档。

附件 2：《保密协议（参考版）》

保密协议

（参考版）

甲方：

注册地址：_____

联系方式：_____

乙方：

身份证号码：_____

联系方式：_____

乙方因在甲方单位履行职务，已经（或将要）知悉甲方的商业秘密。甲、乙双方平等协商，依据《中华人民共和国反不正当竞争法》《四川省反不正当竞争条例》《企业商业秘密保护管理规范》（GB/T 35790-2023）等法律法规，订立本保密协议。双方确认在签署本协议前已详细审阅协议内容，并完全了解各条款的法律含义。

一、保密的内容和范围

甲、乙双方确认，乙方应承担保密义务的甲方商业秘密，涵盖技术信息、经营信息及其他涉密信息，具体范围如下：

技术信息：包括但不限于创新药分子结构、Phase I-III 期临床试验原始数据、生物制剂发酵工艺参数；高端医疗器械核心算法、骨

科植入物材料配方；川产道地药材炮制工艺、中药复方指纹图谱；CAR-T 细胞制备流程、基因编辑工具优化方案、干细胞诱导分化技术参数；微生物细胞工厂构建基因序列、生物基医用材料聚合度调控工艺；手术机器人运动控制算法、机械臂力反馈传感校准参数；海外注册申报资料、国际合作研发的核心技术转移文档等。

经营信息：包括但不限于医保谈判报价策略、带量采购投标预案、区域独家代理合作协议条款、海外市场定价策略；年度研发管线规划（含未公开靶点信息）、与医疗机构合作的临床试验方案、国际合作研发的分工与成本分摊协议；Pre-IPO 轮融资商业计划书（含未公开财务预测）、并购重组标的评估数据、海外子公司运营数据、核心客户名单及交易习惯等。

其他涉密信息：甲方依照法律规定和有关协议约定对外应承担保密义务的事项，以及乙方在履职过程中接触到的甲方未公开的管理制度、流程文件、财务数据等。

乙方确认，前述商业秘密分为核心秘密、重要秘密和一般秘密三个等级，具体等级划分以甲方《商业秘密识别清单》及相关制度为准。

二、乙方的保密义务

主动采取加密措施对上述商业秘密进行保护，包括但不限于遵守甲方数据加密、访问控制、载体管理等技术防护要求，防止不承担同等保密义务的任何第三方知悉及使用。

不得刺探或者以其他不正当手段（包括利用计算机进行检索、浏览、复制等）获取与本职工作或本身业务无关的甲方商业秘密。

不得向不承担同等保密义务的任何第三人披露甲方商业秘密，包括但不限于通过口头、书面、电子传输等任何形式泄露。

不得允许（包括出借、赠与、出租、转让等行为）或协助不承担同等保密义务的任何第三人使用甲方商业秘密。

不论因何种原因终止与甲方的劳动关系，都不得利用甲方商业秘密为其他与甲方有竞争关系的企业（包括自办企业）服务，不得披露、使用或允许他人使用甲方商业秘密。

甲方商业秘密所有权始终全部归属甲方，乙方不得利用自身对甲方商业秘密的了解申请相关所有权（本协议签订前经乙方书面证明已依法具有某些所有权者除外）。

严格遵守甲方关于涉密载体（包括电子文档、纸质文件、实验样本、存储设备等）的管理规定，按要求领用、使用、归还和销毁涉密载体，不得私自留存、复制或转移。

配合甲方开展保密培训、考核、审计等工作，参与泄密应急演练，提升保密意识和应急处置能力。

如发现甲方商业秘密已被泄露或因自身过失导致泄密，乙方应立即采取有效措施防止泄密范围扩大，并在 24 小时内及时向甲方商业秘密保护部门或其指定负责人报告，不得隐瞒。

三、商业秘密的停止使用与载体返还

无论甲、乙双方劳动关系因何种原因终止或解除，乙方应立即停止使用所有甲方商业秘密；只要该商业秘密尚未依法进入公众领域，乙方不得继续使用，也不得向任何个人、法人或其他组织披露。

劳动关系存续期间及终止或解除后，甲方有权随时要求乙方返还从甲方及甲方项目获得的一切涉密资料文件及其复制件、存储载体、实验样本等；乙方应在甲方要求的期限内（最长不超过 7 个工作日）完成返还，或按甲方要求共同销毁，双方签署《涉密载体返还、销毁确认书》。

乙方离职时，应配合甲方开展离职保密审计，完成涉密载体回收、系统权限注销、数据清理等工作，签署《离职保密承诺书》，审计通过后方可办理离职手续。

四、保密期限

本协议约定的保密期限为自协议签署之日起至相关商业秘密依法进入公众领域之日止；若商业秘密始终未进入公众领域，保密期限为永久。

双方劳动关系终止或解除后，乙方的保密义务不受时间限制，仍需持续履行，直至该商业秘密进入公众领域。

若甲方与乙方另行签订竞业限制协议，保密期限与竞业限制期限不一致的，以期限较长者为准。

五、违约责任

若乙方不履行本协议约定的保密义务，应承担违约责任，向甲方支付违约金。违约金数额根据涉密信息的保密等级确定：

泄露核心秘密的，违约金为人民币 50 万元 - 200 万元；

泄露重要秘密的，违约金为人民币 20 万元 - 50 万元；

泄露一般秘密的，违约金为人民币 5 万元 - 20 万元。

若乙方的违约行为造成甲方经济损失（包括但不限于研发投入损失、市场份额损失、许可费损失、商誉损失、维权产生的诉讼费、律师费、鉴定费等），违约金不足以弥补实际损失的，乙方应就不足部分向甲方承担赔偿责任。

若乙方的违约行为给甲方造成不良社会影响和商业信誉损失，乙方还应配合甲方消除不良影响，协助追查、追回流出的涉密信息及载体；无法消除或追回的，甲方有权进一步追究乙方责任。

乙方违反保密义务的，甲方有权根据情节严重程度，采取包括但不限于警告、罚款、调岗、解除劳动合同等内部处理措施；构成犯罪的，甲方将移交司法机关追究其刑事责任。

六、争议的解决办法

因执行本协议而发生的纠纷，双方应首先协商解决；协商不成的，任何一方均有权向甲方所在地有管辖权的人民法院提起诉讼（若涉及技术秘密纠纷，由成都知识产权法院管辖）。

七、协议的效力和变更

本协议自双方签字盖章后生效，取代双方此前就保密事宜达成的任何口头或书面协议。

本协议未尽事宜，双方可另行协商签订补充协议，补充协议与本协议具有同等法律效力。

若本协议条款与国家法律法规或甲方后续修订的商业秘密保护制度相冲突，以国家法律法规及甲方有效制度为准，但本协议其他条款效力不受影响。

（以下无正文，为各方签字页）

甲方（签章）：_____

签署日期：_____年____月____日

乙方（签名）：_____

签署日期：_____年____月____日

附件 3：《竞业限制协议模板（**参考版**）》

竞业限制协议

甲方（用人单位）：

法定代表人：

地址：

联系电话：

乙方（职工）：

身份证号码：

现住址：

联系电话：

鉴于乙方受聘于或服务于甲方，在职或服务期间乙方有从甲方获得商业秘密的机会，有利用甲方物质技术资料进行创作的机会，为切实保护甲方的商业秘密及其他合法权益，确保乙方不与甲方竞业，根据《中华人民共和国劳动法》《中华人民共和国劳动合同法》等法律法规的规定，遵循合法、公平、平等自愿、协商一致、诚实信用的原则，甲乙双方订立本协议供双方共同遵守：

一、有竞争关系的单位范围

单位范围：（根据本单位情况约定乙方不得到哪些单位任职）

地域范围：（根据本单位情况约定乙方不得到什么地方的哪些单位任职）

“有竞争关系”是指与该员工离职时甲方及其关联公司已开展的业务有竞争关系；有竞争关系的单位包括与甲方及其关联公司直接竞争的单位；有竞争关系的地域范围，以能够与甲方形成实际竞争关系的地域为限。

二、限制生产或经营的产品范围和限制从事的业务范围

限制生产或经营的产品范围：（根据单位产品情况而定）

限制从事的业务范围：（根据单位业务情况而定）

地域范围：（根据本单位情况约定乙方不得到什么地方自己生产或经营同类产品和从事同类业务）

三、竞业限制期限及竞业限制义务

乙方在甲方工作期间及乙方从甲方离职之日起_____年内，乙方不得在与甲方及甲方关联公司有竞争关系的单位内任职或以任何方式为其服务，也不得自己生产、经营与甲方及甲方关联公司有竞争关系的同类产品或业务。

乙方在甲方工作期间及乙方从甲方离职后，乙方承担的其他义务包括但不限于：不泄漏、不使用、不使他人获得或使用甲方的商业秘密；不传播、不扩散不利于甲方的消息或报道；不直接或间接的劝诱

或帮助他人劝诱甲方员工或客户离开甲方。乙方履行本条义务，甲方无需给予任何补偿。

乙方从甲方离职时，应提前与甲方确认其是否有离职后的竞业限制义务。甲方如确认乙方有竞业限制必要，应发送《竞业限制开始通知书》，乙方离职后竞业限制义务开始；甲方如确认乙方无竞业限制必要，应发给《竞业限制终止通知书》，乙方无需承担离职后竞业限制义务。

乙方在离开甲方时未提出确认申请的，其离职后竞业限制义务自其离开在

甲方的工作岗位之日起自动开始，竞业限制期内该员工可以向甲方提出竞业限制确认申请，甲方确认乙方有竞业限制必要并发给《竞业限制开始通知书》后，乙方可以开始领取竞业限制补偿金，但在此之前的竞业限制补偿金视为乙方主动放弃。

甲方确认乙方无竞业限制必要时应发给《竞业限制终止通知书》，乙方竞业限制义务终止，在此之前即使乙方履行了竞业限制义务也无权领取补偿金。

四、竞业限制补偿及其支付方式

乙方在甲方及甲方关联公司工作期间履行竞业限制义务，甲方无需给乙方任何补偿。乙方离开甲方及其关联公司后如按照本协议的约定履行了竞业限制义务，甲方应给予竞业限制补偿。

乙方的竞业限制补偿金由甲方按月向其支付，支付日期为当月，每月的数额为乙方离职前_____个月的月平均工资的_____%（计日元）。

乙方领取补偿金时，应向甲方出示当前的任职情况证明，经甲方向乙方工作单位确认后方可领取。乙方逾期一个月未能向甲方提交任职情况证明，视为放弃该月的补偿金。

五、违约责任

乙方违反本协议第二条第（一）项规定的，应立即与甲方竞争单位脱离关系，继续履行本协议，并按照违约期间本合同约定的竞业限制补偿金的_____倍支付违约金。

无法确定违约时间长短的，按照_____年计算，甲方因此而受到的损失大于该违约金的，应赔偿甲方因此受到的全部损失。损失额依照以下三种方式计算，以计算结果最高的为准：甲方获取或开发该产品技术的全部费用；甲方相关业务因此损失的利润；竞争单位相关业务因此取得的利润。

乙方违反本协议第二条第（二）项规定的，应立即停止违约，继续履行本协议，并向甲方支付违约金元，违约金不足以补偿甲方损失的，乙方还应赔偿甲方因此收到的所有损失，计算标准参照前一项规定计算。

甲方逾期支付竞业限制补偿金，应按银行同期贷款利率向乙方支付违约金。

六、其他约定

乙方被新单位录用后应在_____周内将新单位的名称及乙方的职位通知甲方。同时乙方应将自己负有竞业限制义务的情况告知其工作单位。

甲方如认为乙方已无竞业限制必要，有权随时通知乙方终止其竞业限制义务，自通知按乙方提供的地址发出_____日后，乙方竞业限制义务终止，甲方应按照乙方已承担竞业限制义务的时间支付竞业限制补偿金。

乙方可与甲方协商解除竞业限制义务，但乙方不得单方面终止自己的竞业限制义务。

因履行本协议发生争议，双方首先应协商解决，如协商不成，任何一方提起诉讼均由甲方所在地人民法院管辖。《竞业限制开始通知书》、《竞业限制终止通知书》是本合同的附件，与本合同不一致的，以本合同为准。

本合同一式两份，甲乙双方各执一份，自双方签字或盖章之日起生效。

（以下无正文，为各方签字页）

甲方（盖章）：

授权代表人(签字)：

日期：

乙方（签字或盖章）：

日期：

附件 4：《离职保密审计表（参考版）》

成都市生物医疗企业离职保密审计表

审计编号：_____

企业名称：_____

离职员工信息：

姓名：_____

身份证号：_____

所属部门：_____

岗位：_____

涉密等级：☐核心涉密 ☐重要涉密 ☐一般涉密 ☐非涉密入职日期：年____月____日 离职日期：年____月____日离职原因：_____

一、涉密信息接触情况核查

序号	涉密信息类别	具体涉密内容	接触权限	知悉范围	是否已交接	交接对象及日期	备注
1	技术信息				☐是 ☐否		
2	经营信息				☐是 ☐否		
3	其他涉密信息				☐是 ☐否		

序号	涉密信息类别	具体涉密内容	接触权限	知悉范围	是否已交接	交接对象及日期	备注
4	-				□是 □否		

二、涉密载体回收核查

序号	载体类型	载体名称、 编号	数量	回收状态	回收人	回收日期	销毁、 存档情况	备注
1	电子载体	工作电脑（设备编号：_____）						
2	电子载体	加密 U 盘、 硬盘（编号：_____）						
3	电子载体	移动硬盘、其他存储设备						
4	纸质载体	涉密文件、实验记录本（编号：_____）						
5	纸质载体	保密协议、竞业限制协议原件						

序号	载体类型	载体名称、 编号	数量	回收状态	回收人	回收日期	销毁、存档情况	备注
6	实物载体	实验样本、涉密原料（编号：_____）						
7	其他载体							

三、系统权限注销核查

序号	系统名称	账号名称	权限类型	注销状态（□已注销 □未注销 □无需注销）	注销人	注销日期	备注
1	企业 OA 系统						
2	研发数据管理系统						
3	财务系统						
4	CRM 客户管理系统						
5	涉密数据库						
6	其他业务系统						

四、保密协议履行情况核查

核查项目	核查结果	备注
是否签订《保密协议》	□是（协议编号：_____） □否	未签订需说明原因
是否签订《竞业限制协议》	□是（协议编号：_____） □否	签订的需明确补偿标准及期限
竞业限制义务告知情况	□已书面告知（附《告知书》签收记录） □未告知	核心涉密岗位必须告知
离职保密承诺书签署情况	□已签署 □未签署	未签署不得办理离职手续
备注	本项由人事部、商业秘密保护部共同核查	

五、其他审计事项

序号	审计内容	核查结果	备注
1	工作电脑涉密数据清理情况	□已清理（附《数据清理报告》） □未清理	IT 部负责验证
2	外部合作方涉密信息告知情况	□已通知合作方 □无需通知	涉及外部合作的需附通知记录
3	离职前是否存在异常操作（如：大量下载、拷贝涉密数据）	□是 □否	需附 IT 系统操作日志核查结果

六、审计结论与签字确认

审计部门	审计意见	签字	日期
商业秘密保护部	□审计通过 □审计未通过（需补充：_____）		
IT 部	□核实通过 □核实未通过（需补充：_____）		
人事部	□核实通过 □核实未通过（需补充：_____）		
离职员工确认	本人确认已按要求完成涉密信息交接、载体回收及保密义务告知，知晓离职后仍需履行保密义务及竞业限制义务（如有）。签字：_____ 日期：_____		
最终审批意见	□同意办理离职手续 □不同意办理离职手续（理由：）审批人（高管、 部门负责人）： 日期：_____		

填写说明

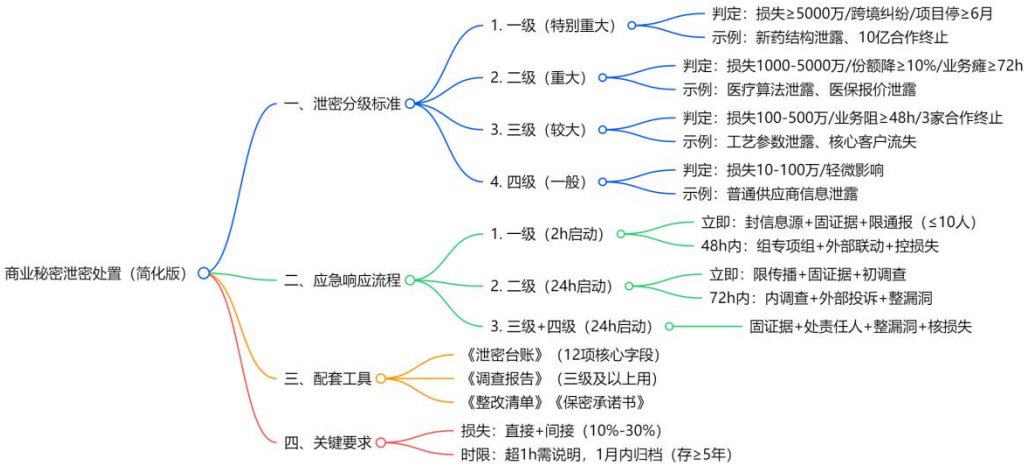
本表格由人事部牵头，联合商业秘密保护部、IT 部共同完成审计，核心涉密岗位需技术部门负责人参与；

各项核查需附对应的附件(如交接清单、注销截图、日志记录等)，作为审计依据；

审计未通过的，需待补充完善相关事项后重新审计，直至通过方可办理离职手续；

本表格一式三份，人事部、商业秘密保护部、离职员工各执一份，存档期限不少于 5 年。

附件 5：泄密时间应急处置流程（参考图及表）



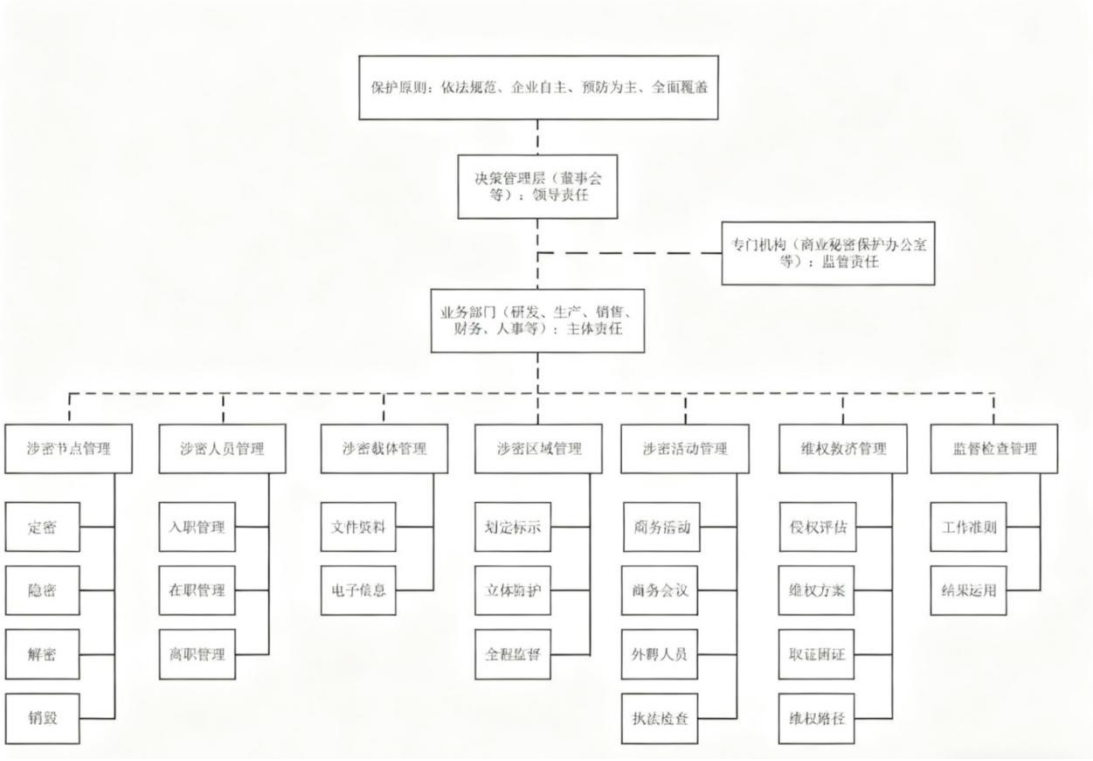
核心模块	一级子分类	二级子分类	三级关键信息（量化、责任、规范）
一、泄密事件分级标准	1. 一级（特别重大）	核心判定维度	- 直接损失≥5000 万元（含研发、市场、维权成本）- 引发跨境纠纷、行业舆情危机- 核心研发项目停滞≥6 个月或终止- 涉密覆盖≥3 个核心业务板块且影响不可逆
		补充细则	核心秘密：企业独有、未公开高价值信息（新药结构、核心算法、独家协议）
		典型示例	- 一类新药结构泄露，研发 2 亿归零- CAR-T 工艺泄露，损失 8000 万- 战略计划泄露，10 亿合作终止
	2. 二级（重大）	核心判定维度	- 核心秘密损失 1000-5000 万；重要秘密损失≥500 万- 重要秘密泄露致市场份额降≥10%（前 12 月均值为基准）- 核心业务瘫痪≥72 小时
		补充细则	重要秘密：影响经营的高价值信息（医疗算法、医保报价、核心工艺参数）
		典型示例	- 医疗算法泄露，损失 3000 万- 医保报价泄露，年损失 800 万- 设备流程泄露，降价损失 1200 万
	3. 三级（较大）	核心判定维度	- 重要秘密损失 100-500 万；一般秘密损失≥100 万- 核心业务受阻≥48 小时或需重大调整- 泄露致≥3 家核心合作方终止合作
		补充细则	一般秘密：可替代的经营信息（非独家客户、常规参数、普通供应商）

		典型示例	- 工艺参数泄露，损失 300 万- 重要客户（年合作≥500 万）流失，损失 450 万- 检测方法泄露，停滞 48 小时损失 120 万
	4. 四级（一般）	核心判定维度	- 一般秘密损失 10-100 万- 仅轻微流程调整、小额成本增加- 涉密为非核心可替代信息
		补充细则	-
		典型示例	- 普通供应商（年合作＜100 万）泄露，损失 50 万- 非核心实验数据泄露，整理成本 30 万- 培训资料泄露，修订成本 15 万
二、应急响应流程	1. 一级泄密（2 小时启动）	立即处置（0-2 小时）	① 封锁信息源（0 小时）：IT + 保密部，断网、冻权限、封载体、限区域② 固定证据（0.5 小时）：IT + 法务 + 公证处，提日志、区块链存证、双人保管③ 内部通报（1 小时）：法定代表人 + 保委会，≤10 人 + 签保密承诺
		48 小时内行动	① 成立专项小组（24 小时）：法定代表人牵头，3 小时内律师到位② 外部联动（36 小时）：报市监局 + 知保中心，跨境联国际机构③ 损失控制（48 小时）：研发调方向、销售停推广、市场监舆情④ 复盘整改（1 周）：3 天出漏洞报告，7 天升级系统 + 培训
	2. 二级泄密（24 小时启动）	立即处置（0-24 小时）	① 限制传播（0-6 小时）：保密部 + 部门，停信息、撤文件、封副本② 固定证据（6-12 小时）：保密员 + IT，区块链存证 + 填登记表③ 初步调查（12-24 小时）：保密部，核范围、锁责任人、出初步报告
		72 小时内行动	① 内部调查（3 工作日）：全流程调查 + 出正式报告② 外部投诉（5 工作日）：报市监局 + 备诉讼材料③ 损失控制（1 周）：调研发、改报价 + 核算损失④ 整改（1 周）：补漏洞 + 升级系统 + 培训
	3. 三级 + 四级泄密（24 小时启动）	24 小时内核心步骤	① 证据固定（0-12 小时）：保密联络员 + IT，填 12 项台账（三级区块链存证）② 内部处理（12-24 小时）：保密部 + 人力，三级约谈、四级警告 + 调权限③ 风险整改（1 周）：查漏洞 + 列整改清单 + 验收④ 损失追责（2 周）：财务部核损失，三级 10%-30% 赔偿、四级 5%-10% 赔偿

三、配套表单工具	1. 《泄密事件台账》	核心字段	事件编号、泄密等级、信息类型、时间、途径、人员、证据、损失、处理、整改、验收、归档号（12 项）
	2. 《泄密事件调查报告》（三级及以上）	核心内容	事件概述、调查过程、证据链、责任人依据、损失测算、处理建议、整改方向
	3. 《整改措施清单》	核心要素	漏洞描述、整改措施、责任部门、责任人、时限、验收标准、验收人
	4. 《保密承诺书》（一级、二级）	核心条款	承诺内容、保密期限、违约责任、签字盖章栏
四、关键补充说明	1. 损失测算标准	公式	直接损失 = 研发投入 + 订单流失 + 维权成本 + 赔偿；间接损失 =（直接损失）×10%-30%（市场、品牌）
	2. 时间节点要求	规范	立即处置超期 1 小时，需向保委会书面说明
	3. 权限管理要求	规则	处置期冻涉事权限，整改后重新评估授权
	4. 归档要求	时限、保存	1 个月内归档，保存≥5 年

附件 6：其他（参考版）

6.1 体系图



6.2 制度要素参考表

制度	要素
商业秘密管理制度	管理目标、管理方针、领导机构、保护要求、资源配备、培训计划、监督检查、评价方案、奖惩措施等
涉密资料、涉密物品管理制度	保护范围、管理单位、使用权限、使用流程、记录存档等
涉密信息系统、云存储空间管理制度	网络安全管理、权限设置、密码管理、定期维护等
涉密区域管理制度	区域划分、出入管理、监控措施、记录存档等
涉密人员管理制度	入职、履职、调岗、离职全过程管理
涉密活动管理制度	活动审批、访客义务告知、保密协议等
商业秘密泄露事件处置管理制度	应急预案、证据收集、维权途径等