

T/SPFRDI

上海市浦东新区研发机构联合会团体标准

T/SPFRDI 005—2025

联合研发中的商业秘密保护指南

Guidelines for trade secret protection in joint research and development

2025 - 8 - 15 发布

2025 - 8 - 15 实施

上海市浦东新区研发机构联合会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 联合研发商业秘密保护基本原则 1

 4.1 最小必要知情原则 1

 4.2 商业秘密分级分类管理原则 2

 4.3 商业秘密联合管理机制原则 2

 4.4 人员全流程管理原则 2

 4.5 商业秘密合规监督与改进原则 2

5 启动联合研发项目前的商业秘密保护管理 2

 5.1 背景商业秘密保护 2

 5.2 背景知识产权尽职调查 2

 5.3 框架协议签订 2

 5.4 保密协议签订 3

 5.5 合作前商业秘密权利管理 3

6 联合研发过程中的商业秘密保护管理 3

 6.1 商业秘密接触人员管理 3

 6.2 背景信息涉密文件的管理 4

 6.3 研发过程中的保密管理 4

 6.4 前景知识产权的保护管理 4

 6.5 研发场所物理管理 4

 6.6 研发设备设施管理 4

 6.7 研发记录与资产管理 5

 6.8 保密监督管理 5

7 联合研发项目终止后的商业秘密保护管理 5

 7.1 前景知识产权的审计与管理 5

 7.2 商业秘密变更协商机制 5

 7.3 项目提前终止的处理机制 6

 7.4 商业秘密信息载体的处理 6

 7.5 项目涉密人员的流动管理 6

 7.6 长期信息共享的渠道和规则 6

8 泄密的纠纷应对处理 7

 8.1 应急处理 7

 8.2 调查取证 7

 8.3 维权途径 7

附录 A（资料性） 商业秘密管理工具表 8

附录 B（资料性） 商业秘密分类（参考） 9

附录 C（资料性） 商业秘密联合管理委员会工作职责 10

参考文献 11

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。

本文件由上海市浦东新区研发机构联合会提出并归口。

本文件起草单位：上海海事大学、上海技术交易所有限公司、上海市浦东新区研发机构联合会、盛美半导体设备（上海）股份有限公司、上海第二工业大学、帕克环保技术（上海）有限公司、上海拜安传感技术有限公司、上海交大智邦科技有限公司、特充（上海）新能源科技有限公司、康码（上海）生物科技有限公司、上海凯鑫分离技术股份有限公司、上海大和衡器有限公司、芯原微电子（上海）股份有限公司、芯原微电子（南京）有限公司、上海达华测绘科技有限公司、上海云晟研新生物科技有限公司、上海芯旺微电子技术股份有限公司、上海境业环保股份有限公司、上海市海华永泰律师事务所、上海规成标准技术服务有限公司、上海新兴科技资讯交流服务中心、重庆汇枫信息科技有限公司

本文件主要起草人：卢长利、宋毅、黄武双、吴毅勋、梁光宇、陆梓语、韩薏卉、王婵婵、胡伟亮、徐海萍、陈钦、郭文艳、田川、白岳松、周涛、罗磊、李欣欣、林怀谷、朱亮、雷先德、刘凯、葛文越、陆陶勤、朱余龙、杨婧楠、周静梅、张岚、高炎、应述欢、王婷婷、丁晓兵、陈晔、张梦婷、顾仲梅、史颖、严芳、郑泽毅、周洁、闫朝

联合研发中的商业秘密保护指南

1 范围

本文件提供了联合研发过程中的从启动联合研发项目前、联合研发过程中以及终止后的商业秘密保护的指导。

本文件适用于具有各类科技创新及自主研发活动的研发主体、需要进行商业秘密风险管理的科研机构和创新型组织在联合研发中的商业秘密管理工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 21374 知识产权文献与信息 基本词汇

3 术语和定义

GB/T 21374界定的以及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。
[来源：中华人民共和国反不正当竞争法，第十条]

3.2

最小必要知情原则 need-to-know principle

仅允许具备实际业务需求的人员接触对应涉密信息，控制信息扩散范围和风险。

3.3

商业秘密分级分类管理 trade secret classification and hierarchical protection

根据涉密信息的敏感程度、影响范围等要素，对商业秘密设定密级并实施差异化保护措施的管理机制。

3.4

背景信息 background information

在联合研发项目开始前，各方已掌握、拥有权属并拟投入项目使用的商业秘密、专利、技术资料等信息资源。

3.5

前景信息 foreground information

在联合研发过程中产生的，具有独立技术、经营价值的成果信息，尚未公开并依法采取保密措施的内容。

3.6

涉密介质/载体 confidential information carrier

承载商业秘密信息的物理或电子介质，如纸质文件、存储设备、代码仓库、原型样机等。

4 联合研发商业秘密保护基本原则

4.1 最小必要知情原则

联合研发各方本着“最小必要知情”的管理理念，对商业秘密知情范围进行严格控制，仅授权具备相应职责或任务需求的人员接触相应涉密信息。信息访问权限应依据岗位职责、任务分工动态设定与调整。

4.2 商业秘密分级分类管理原则

各方根据商业秘密信息的重要程度与敏感性，对其进行分级分类管理。制定相应的分级标准和管理措施，明确不同等级信息的访问控制、传递审批、存储保管和使用限制，详见附录B。

4.3 商业秘密联合管理机制原则

联合研发项目宜建立商业秘密联合管理机制。各方可设立商业秘密联合管理委员会，详见附录C，或指定机构与人员负责协调商业秘密的识别、分类、审批、传递、风险评估与纠纷处理等管理工作。

4.4 人员全流程管理原则

对接触商业秘密的人员，实施从项目参与前到项目结束后全流程的管理制度。管理内容包括但不限于保密协议签署、保密培训、信息访问授权、成果交接、离任交底及后续保密义务的持续约束等，详见附录A。

4.5 商业秘密合规监督与改进原则

各方应建立商业秘密保护的监督机制与风险评估流程，定期检查商业秘密管理措施的执行情况，发现问题应及时整改。

5 启动联合研发项目前的商业秘密保护管理

5.1 背景商业秘密保护

在联合研发前对自身已有商业秘密进行权利归属确认、信息清单编制与载体登记，并设立内部审批机制，针对拟披露的背景信息进行审查，采取适当方式进行背景信息披露。披露过程中宜明确信息的商业秘密属性及披露限制。

5.2 背景知识产权尽职调查

各方宜在合作启动前对所涉及的各方背景技术、商业秘密等进行尽职调查，具体包括：

- a) 识别所有拟投入的背景信息，包括知识产权、技术资料、源代码、工艺参数等。同时核实上述信息的权属状态，清晰界定其可用于合作的范围和条件，明确权利归属、共有人、授权使用记录及保密等级；
- b) 确认是否存在历史转让、许可、开放、发表、合作披露等影响保密的行为；
- c) 审查是否存在法律障碍，包括限制转让、未决纠纷、权属不明等情况；
- d) 分析该项背景信息在预期合作中所起作用及与成果的依赖关系；
- e) 对涉及第三方许可的技术或开源组件进行合规性审查；
- f) 整理形成背景技术信息披露清单，并由各方签字确认，作为合作协议的附件；
- g) 配套提供相关权属证明文件或技术归属声明；
- h) 提交尽职调查报告并纳入合作协议或项目档案备案。

5.3 框架协议签订

联合研发合作在启动前签署框架协议，明确合作目标、信息管理责任及商业秘密保护机制，具体包括以下管理要求：

- a) 明确合作项目的范围、目标、期限、阶段安排及预期技术成果形式；
- b) 约定各方职责分工、技术分工、交付节点、监督机制等管理内容；
- c) 明确各方提供的背景信息，包括商业秘密、专利、技术等信息的范围及使用权利；
- d) 对前景成果的知识产权归属、运营使用权、申请主体等权益进行约定；
- e) 建立联合研发商业秘密管理机制，可设立专责管理委员会或联合管理办公室；
- f) 约定保密条款，明确保密责任主体、信息披露审批流程、监督检查与违约处理机制；

- g) 明确信息分级管理规范，界定不同涉密等级的管理责任和保密技术措施；
- h) 规定合作终止或成果转化后的商业秘密延续保护机制；
- i) 明确适用法律、争议解决方式与保密纠纷处理程序；
- j) 宜附带协议附件，包括背景信息清单、成果分类表、保密义务清单等。

5.4 保密协议签订

为确保信息披露前具备法律约束，各方签署保密协议，其内容包括以下管理要求：

- a) 明确界定本协议项下所称的商业秘密范围，包括技术信息、经营信息、客户信息、财务信息及其他信息，并说明其保密性和非公知性特征；
- b) 明确保密义务主体范围，包括本单位员工、外包人员与第三方机构；
- c) 对涉密信息的传递、查阅、存储、销毁设置管理要求与流程；
- d) 限定商业秘密的用途，仅限于履行项目目标，不得用于其他用途；
- e) 约定保密期限，项目期内与项目结束后的持续保护时间；
- f) 规定违约行为的具体表现形式及相应违约责任承担方式；
- g) 要求采用物理或技术保护措施保障信息安全；

注1：如访问控制、加密、日志追踪。

- h) 明确对外披露的审批流程，涉及向第三方披露时，应履行事先告知义务并明确限制条件；
- i) 建立保密协议履行监督机制与人员变动管理机制；
- j) 可在协议中引用或附带相关附件。

注2：如涉密人员名单（或约定其收集和更新机制）、具体涉密文件清单（或约定其生成和管理机制）及保密说明材料等。

5.5 合作前商业秘密权利管理

合作各方建立清晰的商业秘密权利识别与归属管理制度，特别是在信息提供前，完成以下工作：

- a) 明确拟投入商业秘密的形成过程、关键技术人员与管理责任人；
- b) 确认信息是否来源合法、是否独立形成，避免无权披露他人技术；
- c) 完成商业秘密载体的盘点与归档，宜采用电子数据存证等方式进行证据保全，并办理内部登记手续；
- d) 建立信息传递记录机制，记录何人、何时、以何种方式披露何种信息；
- e) 开展信息敏感性评估，明确哪些属于高风险泄密点；
- f) 确立权属台账制度，将涉密信息与权属单位一一对应，形成台账编号；
- g) 在披露前对文件进行脱敏、加密、水印等处理；
- h) 约定项目过程中新增信息是否归入背景范围，并设立协商机制；
- i) 预设“信息撤回机制”，在必要时允许撤回部分误披露的信息；
- j) 宜由知识产权部门牵头对全部权利归属进行复审与交叉验证。
- k) 宜采用电子数据存证或其他方式进行证据保全，并由责任人签署确认；
- l) 宜定期复核资产清单，尤其在合作启动、中期审查及结项阶段更新一次；
- m) 建立研发资产移交与变更流程，在成果转移、转化前完成手续。

6 联合研发过程中的商业秘密保护管理

6.1 商业秘密接触人员管理

各方对参与项目的涉密人员实施动态、分级管理，具体包括以下内容：

- a) 编制涉密人员清单，明确其接触范围、可访问的商业秘密等级及相应的访问权限，并进行动态更新；
- b) 项目启动前，需对所有涉密人员开展保密义务宣导与专项培训；
- c) 签署岗位级或项目级的保密承诺书，绑定具体职责与信息范围；
- d) 建立涉密人员权限动态调整机制，岗位或职责变动同步更新权限；
- e) 加强对外部参与人员的背景审核，明确管理要求；

注3：如实习生、外包技术人员、外聘兼职专家等。

- f) 宜建立涉密行为日志系统，记录人员查阅、处理、传递商业秘密的关键操作与行为轨迹；
- g) 宜对长期参与项目的人员定期开展保密再培训和纪律考核。

6.2 背景信息涉密文件的管理

各方在联合研发过程中所揭露的背景信息，在文件层面建立从创建、传递、使用到销毁的全流程管理控制机制，具体包括以下内容：

- a) 对涉密文件按密级进行分类；
- 注4：如“限阅”“机密”“核心机密”等。
- b) 为每类涉密文件设定访问控制规则，包括授权对象、查阅方式与审批流程；
- c) 明确传递途径，并严禁通过不合规渠道传输；
- 注5：如加密邮件、专用平台、U盘登记。
- d) 建立涉密文件交付与签收制度，记录文档接收人、时间与目的；
- e) 规定涉密文件使用限制，如不得复制、不得打印、限定查阅时限等；
- f) 采用加密、水印、访问日志等技术手段防止信息泄露与非法复制；
- g) 宜定期检查涉密文件权限分布情况，防范权限扩散。

6.3 研发过程中的保密管理

联合研发活动中的会议、协同工具、成果输出等环节涉及敏感信息交换，建立统一管理制度，具体涉及以下内容：

- a) 设立涉密会议审批流程，明确参会人员、内容分类与会议记录保密等级；
- b) 建立会议纪要加密、限制分享与定期销毁机制；
- c) 规范线上会议平台选择与录音录像管理，敏感内容避免云端存储或转录；
- d) 对项目协同平台设置访问权限与操作日志；
- 注6：如代码仓库、设计系统。
- e) 对中期阶段性成果及时进行保密属性识别与权属认定，不得对外披露、发表或以其他形式泄露；
- f) 要求成果归档同步标记涉密等级；
- g) 宜指定专人担任研发环节“保密联络员”，监督信息产生与传递的合规性。

6.4 前景知识产权的保护管理

项目中形成新的成果在形成阶段采取分类识别的有关管理工作，具体包括以下流程：

- a) 建立成果形成阶段的“成果识别”流程，及时判断知识产权类型以及归属，并依据合作协议约定或内部管理制度进行保护与管理；
- b) 对新成果的保密等级进行初步分级，并指定管理责任人；
- c) 评估该成果是否存在专利保护的可能性，必要时采取“先保密、后公开”策略；
- d) 将具备商业价值的研发记录、关键数据、原型方案等纳入前景商秘管理清单；
- e) 建立项目内部的“前景成果台账”，记录形成过程、人员、载体、归属等信息；
- f) 宜由各方通过协商，就前景成果的权属、使用、许可、披露及保密义务等进行明确约定，并形成书面记录或纳入项目更新协议。

6.5 研发场所物理管理

各方对联合研发使用场所的访问与物理防护实施严格管控，具体采取以下措施：

- a) 对涉密研发区域设置访问权限，采用门禁卡、指纹或人脸识别等方式控制出入；
- b) 在涉密区域入口处张贴显著的保密警示标识，提醒人员遵守保密纪律和访客管理制度；
- c) 对涉密区域内的资料存放、打印设备、摄像头、网络接口等进行定期保密性检查和安全加固；
- d) 禁止携带外部未经登记的移动设备进入涉密区域，应在进入前进行提示，有条件的可配备监控、报警器等；
- e) 对访客设置引导与陪同机制；
- f) 宜定期巡检涉密区域的物理安全状态，及时修复管理漏洞。

6.6 研发设备设施管理

信息系统、研发终端与数据处理工具作为商业秘密流转的关键载体，宜实施技术控制与权限审查，具体包括以下内容：

- a) 对涉及商业秘密相关系统，如文档管理、协同平台，设定角色权限与访问策略；
- b) 要求关键系统启用操作日志、自动备份及异常操作告警功能；
- c) 对个人终端设定登录权限、数据加密与离线处理控制；
- d) 建立研发设备接入登记与退出注销流程，设备调拨需经审批；
- e) 对接入设备的外设使用进行授权或物理隔离；
- f) 宜配套网络隔离、数据防泄漏等技术措施，提升防护水平。

6.7 研发记录与资产管理

合作各方建立健全的研发记录与前期资产登记制度：

- a) 按研发项目、阶段、内容分类建立完整研发笔记、实验记录及核心实验数据等；
- a) 保留自主研发过程中的研发记录与有关文件；
- b) 记录形成的技术资料、样品、数据、设计文件、会议纪要等核心内容；
- c) 宜在记录中标注保密等级与是否拟申请知识产权的信息提示；
- d) 纳入资产清单中列示各类成果及对应权属单位、形成时间、技术负责人等信息；
- e) 对成果资料附加明确的商业秘密标识，并根据需要进行加密处理、权限限定或物理隔离存放；
- f) 同步进行电子化归档，保障远程存取、备份与安全保护；
- g) 可采用电子数据存证或其他方式进行证据保全，并由责任人签署确认；
- h) 宜定期复核资产清单，尤其在合作启动、中期审查及结项阶段更新一次；
- i) 建立研发资产转移与变更流程，在成果转移、转化前完成手续。

6.8 保密监督管理

联合研发项目宜建立内部保密检查机制，对保密制度执行情况与风险点进行常态化评估：

- a) 指定保密管理员或建立联合检查组，开展周期性项目保密合规检查；
- b) 设立保密检查清单，覆盖人员管理、载体交接、设备使用等维度；
- c) 对检查发现的保密漏洞、管理疏漏及违规行为，应建立整改跟踪和闭环管理机制，并定期复核整改效果；
- d) 建立涉密事件发生泄密、失窃或丢失等报告和处置机制，明确报告流程、响应时间、处理责任等；
- e) 宜设立激励或问责制度，对表现突出或失职行为形成可见反馈。

7 联合研发项目终止后的商业秘密保护管理

7.1 前景知识产权的审计与管理

联合研发结束后，宜对项目形成的前景成果及相关商业秘密进行全面审计、归属确认和后续管理安排：

- a) 由联合管理委员会或有关部门开展前景成果清单确认，核查各类成果的权属、使用权限与保密状态；
- b) 确认项目中拟申请专利的成果并进行公开与保密利益权衡评估；
- c) 对前景成果中存在争议或共有情形的，应在项目终止后进一步明确各方的授权、披露、许可和转让规则，或通过协商形成新的合作协议；
- d) 设立成果审计台账，记录成果名称、归属方、合作方使用权、后续运用方向等信息；
- e) 宜明确各类前景成果是否需要继续适用本协议中关于商业秘密保护的延展条款，或另行约定后续保密期限和义务；
- f) 对于不便继续保密保护的成果，可协商确立转为专利、商业化许可等机制，详见 7.2。

7.2 商业秘密变更协商机制

项目终止后，各方就部分商业秘密的属性转化、用途变更等情形建立协商机制：

- a) 设立商业秘密属性变更审议机制，评估是否转为非秘密形式；
- b) 明确申请专利、软件登记或论文发表的前置协商与审批机制；
- c) 协商确定各方对保密成果的再利用、延伸开发权利及其限制条件；
- d) 宜对计划用于产品化、商业化的成果单独设立运营用途协议与披露策略；
- e) 对计划对外投资、设立公司或平台运营的成果，特别审查商业秘密影响及披露合规性。

7.3 项目提前终止的处理机制

在联合研发项目尚未完成时因合作方变更、争议冲突、不可抗力或其他因素提前终止的，妥善开展商业秘密的隔离、清点、协商与控制，防范后续滥用与泄露风险。

- a) 各方于终止决定达成或通知发布后，立即启动信息风险评估与涉密资产清点机制；
- b) 冻结尚未提交或公开的阶段性技术成果，并根据协议确认是否为背景信息、前景成果或争议成果；
- c) 对于已交换但未完成共识确认的信息，各方不得单方面转化、发表、使用或许可第三方；
- d) 各方宜签署联合研发项目终止备忘录或形成书面确认文件，明确商业秘密信息的保密延续义务、载体处理方式与后续禁用约定；
- e) 已授权访问系统、平台的人员账号应同步冻结，并记录权限回收日志；
- f) 分别确认下列事项是否需单独设定后续协议：
 - 1) 部分阶段性成果归属争议协调机制；
 - 2) 尚未转化成果的再利用授权或限制范围；
 - 3) 部分共享成果的分期封存与解密机制。
- g) 如联合研发终止系因一方违约、泄密或其他侵权行为所致，守约方保留依法追究其法律责任的权利，并优先按照合作协议中的争议解决条款进行处理。

7.4 商业秘密信息载体的处理

终止项目后的商业秘密载体需统一处理，确保信息不因分散管理而泄露：

- a) 梳理所有涉密载体，电子、纸质、实物及其流转记录；
- b) 明确由权属方统一接管、加密存档或销毁非必要存续的载体；
- c) 依据协议处理权限问题，区分“返还”、“销毁”、“长期保留”的资料清单；
- d) 出具文件返还、销毁或封存处理的书面凭证并由对方签字确认；
- e) 保留技术档案和信息处理记录，备查与维权使用；
- f) 对于尚有后续合作预期或争议的载体，可约定“封存审阅”状态，并明确重新启动审阅的条件和流程。

7.5 项目涉密人员的流动管理

发生项目涉密人员流动对其权限注销、交接义务和离职后责任作出安排：

- a) 及时注销项目涉密人员的系统权限、访问信息和账号；
- b) 组织项目涉密人员完成商业秘密移交工作，包括载体、文档、原型资料等；
- c) 签署岗位离任保密确认书，重申其对项目涉密信息的持续保密义务；
- d) 对于关键涉密人员，结合岗位风险设立竞业限制或跳槽申报机制；
- e) 告知人员所在单位其保密义务延续时间与不可从事事项；
- f) 对于离职的关键涉密人员，可在合理范围内建立后续监测机制，以发现和制止其可能存在的违规披露或转移商业秘密行为。

7.6 长期信息共享的渠道和规则

对于项目结束后仍需维护的信息协作，事先建立安全的共享机制与规范：

- a) 协商确定需要进入长期共享清单的成果与资料，并就共享范围、使用条件、期限、访问权限等进行详细约定；
- b) 设立专用共享平台或信息传递渠道，限定访问人群与日志记录；
- c) 对共享信息设置有效期、再使用审批机制和技术访问控制；
- d) 约定共享信息使用场景、不得传递第三方或用于竞业事项；

- e) 共享的信息如需进行再加工、集成到其他项目或对外公开，须经包括所有信息提供方在内的全体权利方书面同意。

8 泄密的纠纷应对处理

8.1 应急处理

发生商业秘密泄露或疑似泄露情形时，立即启动应急响应程序，争取第一时间控制风险：

- a) 设立商业秘密应急响应小组，由各方相关部门，包括法务、知识产权、信息安全、技术、管理层等代表组成；
- b) 于事件发生后 24 小时内完成初步核查，并立即启动封堵和防范措施；
- c) 暂停涉密信息访问权限，临时关闭可疑平台或账号入口；
- d) 及时通知合作方，并启动联合会商或应急联络机制；
- e) 形成应急处理报告，记录事件具体情况、处理措施、责任人、后续安排等；
- f) 涉嫌犯罪的，应在固定初步证据后，形成报案材料，并及时向公安机关报案。

8.2 调查取证

商业秘密纠纷处理过程中，证据的完备性直接影响维权成败。应在合法、可用、可举证的前提下保全关键证据：

- a) 保存原始涉密资料版本，包括数据文件、研发记录、电子邮件、系统日志等；
- b) 保全泄密路径信息，包括操作账号、访问权限、传输路径、日志链条等；
- c) 收集涉案人员的岗位职责、接触记录、行为轨迹；
- d) 对电子数据通过公证处、第三方司法鉴定机构、区块链电子数据存证平台进行固定；
- e) 应形成完整证据链条，涵盖权属证明、保密措施、被泄路径及被侵害事实等；
- f) 对于合作外泄密风险，同步保留合同文本、保密协议及传递凭证。

8.3 维权途径

商业秘密遭受侵害后，权利人可依法通过民事诉讼、行政执法、刑事追责等方式维权。企业应结合案情特点选择路径，并严格依照法定程序准备材料、固定证据、控制风险：

- a) 已掌握侵权行为人较清晰的线索，且希望获得赔偿或禁令制止侵权行为，可采取民事诉讼；
- b) 侵权事实清晰、侵权人明确，需快速处理，可采取行政投诉维权；
- c) 泄密行为情节严重，造成重大损失或属于单位犯罪、窃取国家技术成果等，可向经侦有关部门进行报案；
- d) 除上述措施外，还可采取律师函、仲裁、调解等其他综合维权途径。

附 录 A
(资料性)
商业秘密管理工具表

本附录提供包括涉密人员清单、成果清单等在内的商业秘密管理工具表的样例，可结合具体实际工作进行调整。

表A.1 涉密人员基本信息（样例）

序号	姓名	所属单位	部门/岗位	联系方式	参与项目时间	保密资格等级

表A.2 涉密人员分类及权限（样例）

序号	姓名	涉密等级	知悉密集范围	接触涉密信息类型	权限范围（如文件/数据/设备访问权限/区域）	保密期限

表A.3 涉密人员动态管理（样例）

序号	姓名	变更类型	变更内容	变更日期	审批人	备注

表A.4 成果清单与分类（样例）

序号	成果名称	成果类型	完成时间	完成单位	主要贡献人员	密级	备注

附 录 B
(资料性)
商业秘密分类 (参考)

商业秘密主要分为以下几类，具体行业应结合行业与技术特点，梳理自身内部的商业秘密。

表B.1 商业秘密分类参考表

秘密类型	定义	示例
技术信息	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。	产品设计与开发：涵盖新产品的构思、设计图纸、模型，产品的外形、结构、尺寸、材料选择等详细信息； 工艺流程与制造方法：涉及产品生产过程中的各个环节操作步骤、工艺参数、设备运行条件等； 技术诀窍与经验：企业技术人员在长期工作中积累的难以用书面形式完全表达的技术技巧和经验； 软件与算法：企业自主开发的各类软件程序、源代码、算法模型等； 实验数据与研究成果：在产品研发、技术改进过程中产生的实验数据、测试报告、研究论文等。
经营信息	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、招标投标材料、客户信息、数据等信息。	客户信息：企业的客户名单，包含客户名称、联系方式、采购偏好、交易历史、信用状况、交易习惯、意向、内容等信息； 销售与营销策略：销售渠道信息，包括各级经销商、代理商的信息，以及企业开拓市场的独特营销策略，如促销活动策划、广告投放策略、市场定位与细分策略等； 财务信息：企业的财务报表、预算计划、成本核算数据、资金运作计划等； 商业计划与战略决策：企业的长期发展战略、年度经营计划、新业务拓展计划、并购重组计划等； 内部管理制度：企业的组织架构设计、部门职责划分、工作流程与规范、绩效考核制度、薪酬福利体系等； 人力资源信息：员工个人信息（在符合法律法规允许的保密范围内）、员工培训计划、关键岗位人才储备信息、员工绩效评估结果等。
其他信息		

附 录 C

(资料性)

商业秘密联合管理委员会工作职责

联合研发各方可组建商业秘密联合管理委员会，负责开展商业秘密保护、风险防控及合规管理的各项工作。

主要核心职能包括以下内容：

一、制度建设与合规管理

- 1、制定并完善项目商业秘密管理制度，明确密级划分、保密措施、责任追究等规则；
- 2、审核合作协议中商业秘密保护条款，确保符合《中华人民共和国反不正当竞争法》《中华人民共和国保守国家秘密法》等法律法规；
- 3、监督各方落实保密义务，定期评估制度执行效果并提出改进建议。

二、商业秘密识别与分类

- 1、组织技术、法务团队识别项目产生的商业秘密，包括但不限于：
 - 1) 技术信息（如未公开的算法、工艺、实验数据）；
 - 2) 经营信息（如客户名单、供应链数据、成本结构）；
 - 3) 管理信息（如内部流程、决策机制）。
- 2、根据商业秘密的价值、泄露风险及影响范围，划分密级（如“绝密”“机密”“秘密”）。

三、保密措施制定与实施

- 1、物理安全：
 - 1) 划定涉密区域，限制无关人员进入；
 - 2) 对涉密设备、存储介质实施加密、隔离管理。
- 2、技术安全：
 - 1) 部署数据加密、访问控制、日志审计等技术手段；
 - 2) 定期开展网络安全漏洞扫描与修复。
- 3、人员管理：
 - 1) 组织涉密人员签署保密协议，明确脱密期及竞业限制；
 - 2) 开展保密培训与考核，留存培训记录。

四、涉密人员与合作伙伴管理

- 1、建立涉密人员清单，动态更新人员权限与状态；
- 2、审核第三方合作伙伴（如供应商、外包团队）的保密资质，签订保密协议并监督履约；
- 3、处理人员调岗、离职等涉密信息交接，确保无遗留风险。

五、风险监测与应急响应

- 1、定期排查商业秘密泄露风险点（如数据传输、权限滥用、员工违规操作）；
- 2、制定泄密应急预案，明确报告流程、取证措施及责任追究机制；
- 3、发生泄密事件时，立即启动应急响应，协同法务、技术团队采取补救措施，并依法追究责任。

六、争议协调与法律支持

- 1、调解合作各方因商业秘密归属、使用范围产生的争议；
- 2、配合司法机关或行政主管部门调查，提供必要证据材料；
- 3、跟踪商业秘密相关法律法规动态，为项目合规提供法律意见。

七、成果保护与权益维护

- 1、审核项目成果（如专利、商业秘密、软件著作权）的归属与权益分配方案；
- 2、监督成果使用范围，防止未经授权的复制、传播或商业化；
- 3、对侵犯项目商业秘密的行为，协调各方采取法律手段维权。

参 考 文 献

- [1] 全国人民代表大会常务委员会. 中华人民共和国反不正当竞争法（2025年修订）. 2025年
- [2] 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
-