

企业商业秘密保护管理规范

2024 - 12 - 17 发布

2025 - 03 - 17 实施

## 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 总体要求 .....	1
5 组织建设 .....	2
5.1 管理决策机构 .....	2
5.2 办事执行机构 .....	2
6 制度建设 .....	3
7 涉密事项管理 .....	3
7.1 定密 .....	3
7.2 隐密 .....	4
7.3 解密 .....	4
7.4 销密 .....	4
8 涉密人员管理 .....	4
8.1 入职管理 .....	4
8.2 在职管理 .....	5
8.3 转岗、离职管理 .....	5
8.4 竞业管理 .....	5
9 涉密区域管理 .....	6
9.1 物理区域管理 .....	6
9.2 网络区域管理 .....	6
10 涉密载体管理 .....	6
10.1 一般管理 .....	6
10.2 文件资料管理 .....	7
10.3 信息系统管理 .....	7
11 对外合作 .....	7
12 应急处置 .....	8
12.1 应急预案 .....	8
12.2 证据收集 .....	8
12.3 维权途径 .....	8
13 监督检查与评估改进 .....	9
13.1 监督检查 .....	9
13.2 评估改进 .....	9

附录 A (资料性)	企业商业秘密保护考量因素.....	10
附录 B (资料性)	企业商业秘密分类表.....	11
附录 C (资料性)	不侵犯商业秘密承诺函 (参考文本).....	14
附录 D (资料性)	员工保密合同 (参考文本).....	15
附录 E (资料性)	竞业限制协议 (参考文本).....	19
附录 F (资料性)	商务合作保密协议 (参考文本).....	22
附录 G (资料性)	重点行业商业秘密保护要点.....	26

## 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。

本文件由重庆市江北区市场监督管理局提出。

本文件由重庆市市场监督管理局归口并组织实施。

本文件起草单位：重庆市江北区市场监督管理局、重庆市市场监督管理局、北京盈科（重庆）律师事务所、重庆长安汽车股份有限公司、重庆智飞生物制品股份有限公司、重庆登康口腔护理用品股份有限公司、重庆源数聚科技有限公司。

本文件主要起草人：胡健禾、刘庆、聂倩春、张文川、毛宇、许文、张黎、谭明进、谭洋、曾野、安效华、冷丹青、赵丰硕、蔡章利。

# 企业商业秘密保护管理规范

## 1 范围

本文件规定了商业秘密保护的术语和定义、总体要求、组织建设、制度建设、涉密事项管理、涉密人员管理、涉密区域管理、涉密载体管理、对外合作、应急处置、监督检查与评估改进等内容。

本文件适用于企业的商业秘密保护管理。事业单位、研究机构、协会等组织的商业秘密保护管理可参照本文件执行。

## 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

**技术信息** technical information

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。

### 3.3

**经营信息** business information

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。

### 3.4

**涉密载体** secret-related carrier

以文字、数据、符号、图形、图像、视频和音频等方式记录商业秘密信息的各类物质，如纸质文件、磁性介质（例如 U 盘、硬盘、软盘、服务器等）、光介质（例如光盘等）和其他介质。

### 3.5

**涉密区域** secret-related place

含有商业秘密信息、人员进入后可能接触到商业秘密的物理区域或网络区域。

### 3.6

**涉密人员** secret-related personnel

根据工作职责、企业规章制度、保密协议或合作关系等有权接触、使用、掌握、管理涉密信息的企业员工或其他人员。

## 4 总体要求

- 4.1 企业应分析来自国内外的法律法规、技术、竞争、市场、文化、社会和经济环境等外部因素（见附录 A）及企业价值观、文化、知识和绩效等内部因素（见附录 A），建立、实施、持续改进商业秘密保护管理体系。
- 4.2 企业商业秘密保护管理应遵循“依法规范、企业自主、预防为主、全面覆盖”的工作方针。
- 4.3 企业应制定商业秘密管理目标，确定保密、效率、成本三者之间的关系。
- 4.4 企业应将商业秘密保护管理贯彻到企业的全部经营活动中，包括但不限于生产、研发、销售、采购、财务、人事、行政、商业合作等。
- 4.5 企业应制定和实施有关商业秘密的保护、培训、宣传、泄密应急处置和奖惩的管理制度。
- 4.6 企业商业秘密信息的管理应遵循以下原则：
- a) 遵循最小授权原则，根据本企业对商业秘密的分类，对知悉相应商业秘密的授权应控制在最小范围内；
  - b) 遵循必须授权原则，根据本企业对商业秘密的分类，知悉和应用商业秘密必须获得授权，知悉和应用相应层级的商业秘密，必须获得相应层级权限授权；
  - c) 遵循可追溯原则，企业在商业秘密的形成、应用和保护工作中，通过完善记录信息，实现对全过程的追踪。
- 4.7 企业应全面统筹知识产权保护的目的、载体、路径等，将商业秘密与专利、商标、著作权、集成电路布图设计等系统布局，立体保护。
- 4.8 企业宜采取预先存证保护等措施，加强商业秘密前置保护。

## 5 组织建设

### 5.1 管理决策机构

- 5.1.1 企业应设立商业秘密管理决策机构，由企业的董事长、总经理或法定代表人担任机构的负责人。
- 5.1.2 管理决策机构的职责包括但不限于：
- a) 贯彻落实国家有关商业秘密保护的法律法规和规章；
  - b) 确立企业商业秘密保护管理目标、方针；
  - c) 监督、检查企业落实商业秘密保护管理目标、方针情况；
  - d) 做好企业商业秘密保护管理制度体系的评价与改进。

### 5.2 办事执行机构

- 5.2.1 在商业秘密管理决策机构之下设立保密办公室或依托相关部门作为日常办事执行机构，并配备专（兼）职保密员负责企业日常保密工作的开展和保密事务的处理。
- 5.2.2 办事执行机构和保密员的职责包括但不限于：
- a) 制定商业秘密保护管理标准、制度和流程；
  - b) 识别和管理涉密信息、涉密人员、涉密区域、涉密载体；
  - c) 组织企业员工进行商业秘密保护宣传、培训、考核；
  - d) 组织制定、实施商业秘密保护措施；
  - e) 会同各部门对相关保密制度及其落实情况进行检查及督促整改；
  - f) 开展商业秘密泄露的证据整理、搜集、举证、协助调查取证等工作；
  - g) 新闻发布、论文发表、企业标准等信息发布和专利申请前，对涉密信息进行审核。
- 5.2.3 保密员选配条件包括但不限于：
- a) 具备良好的职业道德和职业素养；

- b) 具备良好的保密意识；
- c) 具有丰富的知识积累和较强的管理能力；
- d) 熟悉商业秘密保护法律法规，掌握商业秘密保护基本知识和技能；
- e) 熟悉涉及商业秘密的业务工作和相关管理工作流程。

5.2.4 企业应分析确定企业的商业秘密保护重点部门和重点岗位，划定商业秘密保护重点区域，应在涉及商业秘密保护的重点部门配备保密员。

5.2.5 企业的分支机构、子公司和关联企业可参照设置商业秘密保护机构和专（兼）职保密员。

## 6 制度建设

6.1 企业应坚持业务与保密相结合，按照商业秘密全生命周期安全管理要求，制定商业秘密保护管理制度，并根据实际情况进行评审或修订，企业为建立、实施、保持和持续改进商业秘密保护管理制度提供所需人员、设施、经费等资源保障。

6.2 企业应制定商业秘密保护管理制度，内容包括但不限于：

- a) 商业秘密保护管理组织及职责；
- b) 涉密事项管理；
- c) 涉密人员管理；
- d) 涉密区域管理；
- e) 涉密载体管理；
- f) 对外合作；
- g) 应急处置。

## 7 涉密事项管理

### 7.1 定密

7.1.1 企业应定期对商业秘密进行识别和评估，制定本企业商业秘密保护清单，确定商业秘密保护范围，其表现形式见附录 B，评估范围应包括：

- a) 涉密技术信息：源代码程序、分析方法、计算方法、步骤、算法、数据、计算机程序等与技术有关的信息；
- b) 涉密经营信息：客户信息、成本资料、管理诀窍、经营策略、定价策略、招投标资料、财务信息等与经营活动有关的信息；
- c) 其他符合商业秘密的构成要件，除技术信息、经营信息以外的商业信息。

7.1.2 对企业商业秘密重要性进行核查和评估时应考虑的因素包括但不限于：

- a) 信息的经济价值，包括该信息的现有价值，以及该领域技术革新的速度和有无替代技术等未来价值；
- b) 竞争对手获取商业秘密后产生的价值；
- c) 商业秘密的研发成本以及因信息泄露等可能遭受的损失程度；
- d) 商业秘密泄露后可能承担的法律风险。

7.1.3 企业应根据评估结果将商业秘密信息进行分级管理，实行定期复评、动态调整。

7.1.4 企业应建立商业秘密项目目录清单，确定商业秘密的价值估算、泄露损失、涉密人员范围、保护措施、存放地点及保存方式等内容。

7.1.5 对核查和评估后确定的商业秘密，可通过公证、第三方存证、电子存证等证据保全方式实现对

商业秘密权属的初步确认。

7.1.6 企业应根据商业秘密的内容和密级，确定相关涉密岗位权限和接触商业秘密的范围。

## 7.2 隐密

7.2.1 企业在进行生产、经营、宣传、商务活动时，应对商业秘密信息予以隐藏，可采取的隐藏方式包括但不限于：

- a) 隐藏或删除涉密信息；
- b) 对涉密信息进行模糊化处理；
- c) 对涉密信息进行加密处理。

7.2.2 配合行政机关和部门的行政检查、行政执法行动如涉及商业秘密的，企业应主动告知。

## 7.3 解密

7.3.1 企业的商业秘密出现下列情形时，可予解密：

- a) 企业认为商业秘密事项已不再具有保护价值的；
- b) 保密期限届满；
- c) 其他特定因素导致商业秘密被公开的。

7.3.2 可采取的解密方式包括但不限于：

- a) 移出涉密区域；
- b) 消除密级标识、提示；
- c) 电子文档解密。

## 7.4 销密

7.4.1 企业销毁涉及商业秘密的文件资料、载体和物品，应经本企业商业秘密保护部门审批后实施，并确保销毁过程得到有效监督且被销毁载体或物品无法被有效复原。

7.4.2 可采取下列方式对销毁过程进行监督管理：

- a) 在视频监控范围内销毁；
- b) 不少于2名员工见证下销毁；
- c) 对销毁过程录像。

7.4.3 可采取的销毁方式包括但不限于：

- a) 文件、资料应粉碎成颗粒状或焚烧处置；
- b) 电子信息应利用彻底删除软件永久删除；
- c) 含有商业秘密的电子信息载体应做销毁处理。

## 8 涉密人员管理

### 8.1 入职管理

8.1.1 涉密重点岗位员工入职前应做背景调查，接触过第三方商业秘密可能产生纠纷的，应签订不侵犯商业秘密承诺函（见附录C）。

8.1.2 新入职、转岗到涉密岗位的员工，应与其签订与岗位工作内容相适应的员工保密合同（见附录D）。

8.1.3 在录用潜在竞争性关系企业的员工时，宜采取的措施包括但不限于：

- a) 审核待录用的员工与原企业之间的保密约定、保密义务、保密内容及范围；



- b) 提醒待录用的员工不应将原企业的商业秘密带入本企业进行使用或公开；
- c) 定期对已入职的员工所从事的业务内容进行审核。

## 8.2 在职管理

8.2.1 企业应将员工商业秘密保护培训列入年度培训计划，可采取发放资料、集中培训、网络培训等方式开展培训，保存培训记录。

8.2.2 企业应督促员工做好本岗位商业秘密保护工作，包括但不限于：

- a) 涉密信息及载体应及时标记，建立管理台账；
- b) 使用涉密信息应履行登记手续；
- c) 涉密电子文档、数据按规定途径和要求使用、流转等；
- d) 离开工作岗位前及时下线工作账户，或设置电脑锁屏等。

8.2.3 企业应采取适当措施防止员工未经授权出现下列行为，包括但不限于：

- a) 登陆未授权账户或系统；
- b) 利用系统漏洞以不当方式获取涉密文件资料、物品、数据；
- c) 超范围、超权限获取使用涉密文件资料、物品、数据；
- d) 复制、发送涉密电子文档；
- e) 将涉密电子文档存储于未授权载体或网络空间；
- f) 拍摄、摘抄涉密资料；
- g) 拍摄、测绘、仿造涉密物品；
- h) 进入非授权涉密区域；
- i) 披露企业未公开的信息。

## 8.3 转岗、离职管理

8.3.1 涉密岗位员工转岗、离职前，企业应告知其不应有下列行为，包括但不限于：

- a) 复制、带离、损毁、篡改、拍摄涉密文件资料、物品；
- b) 查阅、拷贝、篡改、发送涉密电子文档、数据；
- c) 删除、更改账户；
- d) 披露、使用或允许他人使用商业秘密。

8.3.2 企业宜对涉密岗位员工采取脱密期管理，及时回收权限，并开展离职检查，进行书面记录，检查内容包括但不限于：

- a) 办公软件、信息数据访问日志是否有异常，如异常查询、拷贝、下载、修改、删除、复制痕迹等；
- b) 是否有对外发送商业秘密信息的记录；
- c) 是否有权限之外的技术文档、信息数据等；
- d) 离职前一定期限内的涉密文档、数据的查看和使用情况等。

## 8.4 竞业管理

8.4.1 企业应设置竞业管理机制，机制应覆盖在职、离职人员竞业管理工作。

8.4.2 企业应对董事、高级管理人员、核心技术人员及其他涉密人员进行竞业评估，与其签订竞业限制协议（见附录 E），内容应包含但不限于：竞业范围、竞业期限与区域、竞业行为、违约责任、补偿金条款等。

8.4.3 企业对离职人员应建立竞业监督机制，及时掌握离职员工在竞业限制期限内的任职去向。

## 9 涉密区域管理

### 9.1 物理区域管理

9.1.1 企业内部的办公区域应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。涉密区域可包括核心产品或服务的研发、生产场所，存储商业秘密信息的数据中心、档案中心等。不同密级的区域之间应采取物理门、墙、隔断等物理隔离措施。密级高的办公区域应设置在离企业出入口相对较远的位置。

9.1.2 涉密区域可采取下列保密措施，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) 不应携带手机、便携机、平板、智能手表等具备拍摄、录音、存储功能的设备器材；
- e) 不应让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。

9.1.3 企业应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，非经审批不应允许外部人员进入内部区域或涉密区域办公。

### 9.2 网络区域管理

9.2.1 企业宜按照业务系统及技术防护软硬件系统需要建设内部网络，并设置有合理的设备冗余，保证网络及网络设备处理及吞吐能力可满足业务和安全需要。

9.2.2 企业应根据业务和保密要求，将内部网络划分为不同访问权限的区域，根据访问控制策略设置访问控制规则。

9.2.3 涉密网络区域可采取下列保密措施，包括但不限于：

- a) 不接入外网；
- b) 与其他内部网络隔离，相互不连通；
- c) 与其他内部网络采取不同的分级管理措施；
- d) 不使用无线网络、无线热点；
- e) 访问涉密区域网络的设备设置终端准入限制；
- f) 通过 VPN 等方式远程接入涉密区域网络，设置终端准入、身份安全等验证措施；
- g) 配备独立的网络基础设施，如服务器、防火墙、专线。

## 10 涉密载体管理

### 10.1 一般管理

10.1.1 企业应对涉密载体的制作、使用、复制、保存、维修、销毁等过程实施全生命周期管理。

10.1.2 企业应采取标记、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。

10.1.3 企业应对能够接触、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。

10.1.4 企业应对涉密载体实行编号管理、分部门管理等保密管理方式。

## 10.2 文件资料管理

10.2.1 应有密级、保密期限等标识，实行登记管理、归档存放。

10.2.2 由部门保密员登记造册，按权限使用，查阅、借阅、续借应履行登记手续。

10.2.3 复制（复印、打印、扫描、拍摄、摘抄等）、跨区域转移、向第三方披露或提供第三人使用前应履行审批和登记手续，复印件或复制件与原件的密级、保密期限相同。

## 10.3 信息系统管理

10.3.1 应对设备、数据库和应用系统及其账户实行权限管理，按岗位职责或特定工作事项按“最小授权”原则设定权限，权限到期、人员转岗、项目或事项变更时应重新授权。

10.3.2 应充分考虑设备、数据库和应用系统的安全性，并满足下列要求：

- a) 做好病毒防范和病毒库的升级、查杀病毒等工作；
- b) 定期进行安全检查，发现系统漏洞及时修补；
- c) 用户的操作行为应有日志记录，可实时报告登陆、获取信息和异常入侵等行为。

10.3.3 应对设备、数据库和应用系统设置账户和密码，并满足下列要求：

- a) 不应使用默认密码或保存密码自动登陆；
- b) 应根据企业的业务类型，采取适当的账户、密码管理方式；
- c) 应对所有涉密账号和密码实行统一登记、备案、发放和变更管理。

10.3.4 涉密数据的存储与使用满足下列要求：

- a) 应存储于企业授权的存储设备和应用系统；
- b) 应采用加密方式存储，指定专人进行解密操作；
- c) 员工应按照权限使用加密数据，超出权限查阅或使用加密数据的，应履行审批手续；
- d) 在查阅或使用完成后，应彻底删除，不应非工作需要而擅自使用。

10.3.5 涉密数据的收发与复制满足下列要求：

- a) 收发涉密数据应经过审批，并采取加密措施；
- b) 传输涉密数据应通过内部局域网或加密网络通道完成，内部局域网应与互联网隔离；
- c) 涉密数据应加密和签名，可限定编辑权限、打开次数和时限等；
- d) 应对涉密数据拷贝采取限制措施，妥善保存拷贝记录。

10.3.6 涉密信息使用云储存时，企业应严格考察其保密性、安全性、稳定性，并对使用权限、网络服务配置要求、专用设备要求、使用记录监察要求等事项与平台运营商作出明确约定。

## 11 对外合作

11.1 在采购、销售、参展等对外商务合作中，企业应采取下列措施，包括但不限于：

- a) 在开始商务谈判前或提供涉密信息前，与对方签署商务合作保密协议（见附录 F）；
- b) 在参展过程中通过遮挡、与展览方签订保密协议等方式降低泄密风险；
- c) 对协议履行过程中涉密信息的使用情况及泄漏情况进行监督管理；
- d) 保留商务合作中商业秘密管理的成文信息。

11.2 在委托开发、合作开发、定作承揽等对外技术合作中，企业应采取下列措施，包括但不限于：

- a) 充分了解合作方的商业秘密管理能力；

- b) 在技术合作中应采取措施防止侵犯他人商业秘密，商业秘密所有人应承诺其商业秘密不侵犯第三方任何权利；
- c) 约定背景商业秘密和共同开发、改进或二次开发中涉及商业秘密的内容和归属，必要时可对保密内容签署单独的保密协议；
- d) 保留技术合作中商业秘密管理的成文信息。

11.3 保密协议应明确保密要求，约定保密内容和范围、保密责任和义务及违约责任，对涉及商业秘密等知识产权的权利归属和使用权做出约定。

## 12 应急处置

### 12.1 应急预案

12.1.1 企业应制定泄露和侵犯商业秘密事件的紧急处理应急预案，预案内容包括但不限于：

- a) 防止信息进一步扩散或损失扩大的保护措施，将危害和损失控制在最小限度内；
- b) 商业秘密泄露的核查、确认和评估方案，查明原因、责任人；
- c) 证据收集、固定方案；
- d) 启动内部处罚和外部维权方案。

12.1.2 企业应培训和引导员工对商业秘密可能泄露的异常状态保持警觉，发现可能泄密迹象及时报告。

### 12.2 证据收集

企业指称他人侵犯其商业秘密时，应及时收集相关证据，包括：

- a) 拥有的商业秘密符合法定条件，证据包括：
  - 1) 不为公众所知悉的证明或鉴定，
  - 2) 商业价值和造成的损失，
  - 3) 对该项商业秘密所采取的具体保密措施，
  - 4) 商业秘密的载体和具体内容，商业秘密权属证据（包括研发或受让等相关资料）；
- b) 与本企业商业秘密相同或者实质相同；
- c) 涉嫌侵权人的主体信息；
- d) 涉嫌侵权人接触或有可能接触本企业商业秘密；
- e) 涉嫌侵权人采取不正当手段。

### 12.3 维权途径

12.3.1 企业的商业秘密被侵犯，可依法采取下列方式进行维权：

- a) 向市场监督管理部门举报；
- b) 向仲裁机构申请仲裁；
- c) 向人民法院提起民事诉讼；
- d) 向公安机关报案；
- e) 向人民检察院申请法律监督等。

12.3.2 涉及国家秘密的，应立即采取补救措施，并向当地公安机关、国家安全机关和保密行政管理部门报告。

12.3.3 企业在依法维权过程中，应防止商业秘密的二次泄露。

## 13 监督检查与评估改进

### 13.1 监督检查

13.1.1 企业应对商业秘密保护管理制度落实情况开展监督检查，监督检查方案应包括：

- a) 监督检查工作的内容和方法；
- b) 监督检查工作的职责和权限；
- c) 执行监督检查的频次和时限；
- d) 监督检查结果运用的整改、问责、奖惩机制。

13.1.2 监督检查内容应包括：

- a) 商业秘密的定密、隐密、解密、销密情况；
- b) 涉密人员管理情况；
- c) 涉密区域管理情况；
- d) 涉密载体管理情况；
- e) 对外合作管理情况；
- f) 企业认为其他应列为监督检查的内容。

13.1.3 监督检查方法宜包括：

- a) 调取涉密纸质文件使用记录；
- b) 调取涉密电子信息载体、信息系统、云存储空间使用记录；
- c) 调取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) 调取涉密活动记录及附属合同。

### 13.2 评估改进

13.2.1 企业应根据监督检查结论评价商业秘密保护管理情况，并形成评价报告，报告内容包括：

- a) 制度是否得到有效实施；
- b) 商业秘密安全与否的客观程度；
- c) 应对风险所采取措施的有效性；
- d) 商业秘密保护管理制度改进的需求。

13.2.2 企业可根据自身情况，委托第三方专业机构对企业商业秘密保护管理情况进行评价，第三方专业机构应如实记录，并形成评价报告，提出改进意见。

13.2.3 企业应针对评价报告发现的问题制定整改计划，采取有效措施持续改进。

13.2.4 企业应对商业秘密保护制度落实环节中存在的问题对责任人进行约谈、问责。

13.2.5 企业应对改进情况定期进行复查、复评。

**附录 A**  
**(资料性)**  
**企业商业秘密保护考量因素**

**A.1 外部因素**

A.1.1 企业应分析来自国内外的法律法规、技术、竞争、市场、文化、社会和经济环境等外部因素。

A.1.2 由于外部因素会影响或潜在影响企业的商业秘密保护责任和能力，因此企业应确定：

- a) 在开展商业秘密保护有关的工作充分考虑以下因素，包括但不限于：顾客、供方、合作伙伴、员工的原企业、竞争对手、技术发展、网络安全、社会文化、监管部门等；
- b) 与商业秘密保护有关的要求力求全面，包括但不限于：商业秘密的诉讼要求、合同中关于保守商业秘密的约定、员工与原企业签订的保密协议等；
- c) 监测和评审外部因素的信息及其相关要求。

**A.2 内部因素**

A.2.1 企业应分析企业价值观、文化、知识等内部因素，并按照相关标准的要求及自身的需要，建立、实施、保持和持续改进商业秘密保护管理体系。

A.2.2 企业在实现商业秘密保护的过程中应考量商业秘密保护管理体系所需的要素及其在整个企业中的应用和对企业商业秘密保护的影响，应考量如下因素：

- a) 确定商业秘密保护所需的输入和期望的输出；
- b) 确定商业秘密保护的顺序和作用；
- c) 确定和应用商业秘密保护所需的准则和方法（包括监视、评价和相关绩效指标），以确保过程的有效运行和控制；
- d) 确定商业秘密保护过程所需的资源并确保其可获得；
- e) 分配商业秘密保护过程的职责和权限；
- f) 按照自身的要求应对风险和机遇；
- g) 评价商业秘密保护过程，实施所需的变更，以确保实现过程的预期结果；
- h) 改进过程和商业秘密保护管理制度。

A.2.3 企业应定期对内部因素的相关信息进行检测和评审。

**附录 B**  
**(资料性)**  
**企业商业秘密分类表**

企业商业秘密分类表见表 B.1。

**表B.1 企业商业秘密分类表**

项目	核心商密	普通商密
经营战略信息	1. 战略决策； 2. 经营计划； 3. 股东会、董事会和监事会会议记录； 4. 合资合作协议； 5. 重大项目审批； 6. 投资项目的有关材料：投资意向书、评估报告、谈判期间来往材料、被投资企业股东协议及财务报表、可行性研究报告、项目建议书和企业对外投资决议等。	1. 管理层会议、其他会议的会议纪要及上述议定的不宜公开的或议定尚未公开的事项； 2. 查处违纪案件的请示、报告、内部讨论情况，办案过程中收集掌握的各类证据，以及未公布的调查报告、处理决定和内部通报；违纪案件的举报人和证人的姓名、住址以及可能危害其安全的有关材料。
规章制度	—	1. 带有涉密信息的规章制度； 2. 企业各级财务、人事、劳资、营销和生产等部门专业性会议材料，以及上述未议定的事项或议定尚未公开的事项。
人事信息	—	1. 人事方案（如人员任免方案、人事安排方案及录用考核标准）； 2. 员工薪酬，包括尚未公布的企业工资制度改革、调整工资方案和实施办法； 3. 离职资料； 4. 绩效考核资料； 5. 员工档案（如员工简历、面试记录、员工证件，员工收入等）； 6. 带有涉密信息的培训资料； 7. 处理劳动工作中重大突发事件或不安定因素的对策及正在调查中的职工安定因素的对策及正在调查中的职工伤亡事故案情。
财务信息	1. 尽职调查报告、投资并购和股权类投资报告； 2. 经营计划、年度预算滚动经营预测及绩效回顾； 3. 董事会议案（财务部分）； 4. 关联交易报告； 5. 生产成本信息； 6. 贷款及抵押信息；	1. 账务账册、凭证； 2. 会计报告、报表； 3. 税务信息； 4. 资金报表； 5. 业务类合同及协议； 6. 企业负债情况；

表 B.1 企业商业秘密分类表（续）

项目	核心商密	普通商密
财务信息	7. 网银支付密码； 8. 银行预留印鉴； 9. 项目审计档案。	7. 与政府签订的合同及协议； 8. 风险管理报告。
业务信息	1. 企业发展规划、计划、设想以及市场战略； 2. 市场调查报告（市场动向，顾客需求、价格、其他企业动向及对这些情报的分析方法和结果）； 3. 新产品投放市场时间、价格策略、产品市场占有率情况及如何开拓新市场、产品的社会购买力情况、产品的区域性分布情况、产品的长中期发展方向和趋势、经营战略、销售流通渠道等； 4. 营业战略（有关和其他企业合作销售、销售途径的确定及变更，对代理商的政策等情报）； 5. 客户数据库信息（客户名单、各相关职位联系人员及联系方式、销量、占客户采购量份额、价格及其设定方法和基准）。	1. 客户信息（资信情报、经营状况）； 2. 行业市场信息分析； 3. 招投标中的标底及标书内容； 4. 营销计划（通过促销等手段强化营销能力、营销区域及选定上市期）； 5. 一般的业务合同（如贸易合同、佣金合同、服务合同、商务单据等）； 6. 退货和投诉处理（退货的品名、数量、原因及对投诉的处理方法）； 7. 销售提成； 8. 招投标中的标底及标书内容； 9. 供应商信息； 10. 合同与订单； 11. 采购计划、采购价格、采购数量； 12. 原材料供应报表； 13. 供应商信息； 14. 授信客户资信报告。
技术信息	1. 研发战略资料； 2. 产品项目组实验记录和实验结果、工艺配方、样品、数据、加工技术、工艺、技改方案、重要课题的分析方法等； 3. 重要科研课题的选项、立项。已立项的科研项目的总体方案、研究资料、成果预测； 4. 尚未公开的企业科研成果资料和论文； 5. 重要产品的开发计划、设计方案、实验过程、生产工艺和关键技术； 6. 施工图纸、设计文件及试车文件； 7. 扩初设计材料、竣工资料； 8. 技术类会议纪要； 9. 非土建类专用笔记本； 10. 生产工艺步骤的工艺参数文件； 11. 生产工艺步骤的生产指导类文件； 12. 生产工艺步骤的生产记录文件； 13. 生产工艺步骤的设备资料； 14. 中试文件； 15. 中控技术标准、中控分析汇总表； 16. 技改文件；	1. 日常管理记录本； 2. 新产品开发计划和试制进度安排（如新产品开发人员的组成、业务分工、技术人员的配置等）； 3. 产品项目组文献资料； 4. 签订的各种合同文本，合同规定不得对第三方泄露的及从技术转让方进来的有关技术转让的所有的材料（包括磁带、图纸、软件等）； 5. 分析项目组实验记录、分析报告、仪器操作规程及文献资料； 6. 产品技术文件包括产品规范、质量标准、测试规范和方法、验收标准、技术水平、技术潜力、新技术前景预测、替代技术的预测、新技术影响的预测及产品合格率、缺陷密度、合格率分析数据、产品验收的数据分析材料等； 7. 项目人员奖励； 8. 易制毒化学品相关资料； 9. 实验设备资料；



表 B.1 企业商业秘密分类表（续）

项目	核心商密	普通商密
技术信息	17. 重要科研项目文件； 18. 涉及生产成本、经营管理数据的日月报表； 19. 工艺技术类的会议和日志文件； 20. 月度、季度、年度生产计划及承包方案； 21. 工艺车间的原材料物流账目。	10. 设计和开发控制程序相关资料； 11. 项目管理制度、审批材料； 12. 招投标资料； 13. 商务合同； 14. 非技术类会议纪要； 15. 土建类专用笔记本； 16. 非工艺的生产指导类文件； 17. 非工艺的生产记录文件； 18. 非工艺的设备资料； 19. 其他生产计划类文件； 20. 其他统计报表类文件； 21. 体系类文件； 22. 质检类文件； 23. 非工艺技术类的会议和日志文件。
软件信息	企业内部办公自动化和业务管理中使用的各类计算机系统资料、数据库、程序命令和密码。	软件序列号。
法律事务	1. 重大诉讼、仲裁事项； 2. 尚未发布的专利申请材料、专利动向； 3. 不对外公开的尽职调查信息。	1. 日常诉讼或其他有争议案件； 2. 各类纠纷（民事、无形资产、工伤、离职等纠纷的内容）； 3. 股权变更交易材料； 4. 不对外公开的企业或子企业设立、注销材料； 5. 保险、专利及其他重要合同。

附 录 C  
(资料性)  
不侵犯商业秘密承诺函 (参考文本)

承诺人姓名: \_\_\_\_\_

身份证号码: \_\_\_\_\_

鉴于本人在入职公司前接触过第三方的商业秘密, 为避免因此可能产生的纠纷给公司造成不应有的损失, 特此承诺如下:

一、本人完全知悉并遵守与任何第三方之间的关于商业秘密保护的法定或约定之义务, 尊重第三方合法享有的商业秘密等知识产权。

二、本人未以不正当手段获取第三方的商业秘密, 未经授权不会披露、使用或允许他人使用第三方的商业秘密, 包括但不限于: 不携带第三方商业秘密信息载体进入公司办公场所; 不使用公司设备存储第三方商业秘密信息; 不通过公司网络、通讯工具传输第三方商业秘密信息; 工作中不使用第三方商业秘密信息。

三、本人不会以任何形式侵害第三方的技术秘密自行申请专利, 或将第三方的技术秘密提供给公司用于申请专利。

四、如因本人侵害第三方的商业秘密产生的法律责任由本人自行承担; 如因本人侵害第三方商业秘密对公司造成损失的, 由本人向公司赔偿相应损失。

(以下无正文)

承诺人:

年 月 日

**附 录 D**  
(资料性)  
员工保密合同（参考文本）

合同编号：XXXX 保密合同[ ] 号

甲 方（用人单位）：\_\_\_\_\_

统一社会信用代码：\_\_\_\_\_

住所地：\_\_\_\_\_

乙 方（劳动者）：\_\_\_\_\_

身份证号码：\_\_\_\_\_

联系电话：\_\_\_\_\_

现居住地址：\_\_\_\_\_

乙方知悉甲方是商业秘密权利人，自愿为其因工作而知悉的商业秘密对甲方承担保密义务，甲、乙双方在自愿、诚实信用原则下，经充分协商，达成如下一致条款，并共同恪守。

**第一条 入职告知**

1. 乙方在进入甲方工作单位之前，应如实披露是否与曾经工作过的任何单位或合作单位签署了保密协议，是否掌握了曾经工作过的单位的商业秘密。

2. 乙方如因曾经签订相关保密协议、竞业限制协议而承担有相应的保密义务及竞业限制义务的，乙方应保证：

(1) 严守遵守其前工作单位或合作单位的保密义务，在甲方工作期间不泄露、不使用其在前单位掌握、知悉的商业秘密；

(2) 如实向甲方告知与其前工作单位签订的保密协议、竞业限制协议具体内容；

(3) 在甲方工作期间不违反与其前工作单位的竞业限制约定，不得利用前单位的商业秘密从事与其前工作单位具有竞争性质的业务工作。

**第二条 商业秘密范围**

甲方的商业秘密范围是指甲方不为公众所知悉、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，也包括甲方依据法律规定及合同的约定对第三方承担了保密义务的第三方的技术信息和经营信息。

技术信息主要包括：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、图纸设计方案等信息。

经营信息主要包括：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。

甲方的商业秘密包括且不限于甲方管理文件等资料载明的商业秘密保护范围，包括且不限于特定的、完整的、部分的、个别的不为公众所知悉的商业信息或未披露的信息，包括且不限于涉及商业秘密的草稿、拟稿、草案、样品、图形、三维、模型、文档、文件、数据、资料等商业信息。

### **第三条 乙方对商业秘密保护的义务**

乙方已充分认识到保守甲方商业秘密是关系到公司生存和发展的重要问题，乙方应严守甲方的商业秘密，并自愿承担保密义务，除因工作需要且经甲方商业秘密保护部门批准，向应该知道前条所列之商业秘密内容的甲方客户或第三人进行必要的保密性交流之外：

1. 严格遵守甲方制定的涉及商业秘密保护的制度；
2. 不得在与甲方有竞争关系的企业兼职；
3. 不得直接或间接向甲方内部无关人员泄露；
4. 不得直接或间接向甲方外部的单位或人员泄露；
5. 不得为自己利益使用或计划使用；
6. 不得擅自复制或披露包含甲方商业秘密的文件或文件副本；
7. 不得擅自拷贝甲方计算机软件的任何数据、文件资料或信息；
8. 对因工作所保管、接触的甲方客户提交的文件应当妥善保管和管理，未经商业秘密保护部门批准，不得超出工作范围使用；
9. 发现第三人以盗窃、贿赂、欺诈、胁迫、电子侵入或其他不正当手段谋取或计划谋取甲方商业秘密时，即向商业秘密保护部门报告，并积极采取保护的必要措施；
10. 其他应当承担的保密义务。

### **第四条 成果归属和报告义务**

1. 乙方因工作、职务或者主要利用甲方的条件、设施等而创造和构思的有关技术和经营的商业秘密权属归甲方所有；乙方为甲方公司利益而作出职务成果时，应当在作出之日起 10 天内向甲方商业秘密保护部门报告。

2. 乙方在职期间或离职一年之内的非职务发明，应以书面形式向甲方提交非职务发明的材料，经甲方确认的非职务发明，其所有权、使用权与甲方无关。

## 第五条 职务成果的奖励

甲方制定职务成果奖励规定可作为本合同的重要组成部分，并遵照执行。

## 第六条 乙方承诺

乙方承诺在甲方工作期间，严格遵守本合同第三条的保密义务，并不得实施以下行为：

1. 将自己使用的电脑用户名、密码告诉第三人，对电脑页面或内容进行拍摄、摄像，非法获取电子数据商业秘密，以电子侵入或非法侵入方式使用电脑、获取存储的商业秘密或信息；
2. 与甲方有交易关系或竞争关系、行业相同或相似的国内外任何企业进行交易，或由亲戚朋友名义进行交易或变相交易；
3. 组建、参与组建或投资、变相投资与本合同第二条甲方经营相关、相同或相似的企业；
4. 直接或间接或帮助第三人劝诱掌握甲方商业秘密的人员离开甲方；
5. 直接、间接或者试图影响侵犯甲方拥有的客户名单及其客户关系的商业秘密，包括客户名称、联系人、联系人习惯、联系方式、聊天工具、电子邮箱、交易习惯、合同关系、合同内容、佣金或折扣、交提货方式、款项结算等；
6. 利用非工作时间为与甲方同行业的企业工作、提供咨询服务等；
7. 采取其他不正当手段。

乙方无论以任何原因离职或解除劳动关系后，仍然无条件地对甲方商业秘密承担保密义务，直至该商业秘密完全公开。

## 第七条 保密材料的交还

1. 乙方无论何种原因离开甲方，均应当自觉办理离职手续、接受甲方组织的离职前保密谈话，并交还甲方本合同第二条所列属于甲方商业秘密的所有文档、数据、三维、文件、资料（包括电脑、硬盘、U盘、光盘、软盘等存储载体中的信息）、物品等。
2. 乙方个人工作日记中含有甲方商业秘密的，应当同时交还或由商业秘密保护部门监督销毁。
3. 甲方应当列出乙方掌握甲方商业秘密的清单，双方确认、签字，并办理交还的交接手续。经过三次以上书面通知（包括不限于法务函、短信、律师函等），仍然不移交商业秘密的，进行失信公示。
4. 若乙方擅自带走或不予交还的，视为盗窃商业秘密的行为。

## 第八条 合同有效期限

1. 上述保密义务对乙方长期有效，无论其在职期间，还是离职之后，除非甲方商业秘密为公众所知悉或完全公开；
2. 因乙方的过错导致甲方商业秘密进入公知领域，即使甲方追究了乙方相关的法律责任，乙方仍无权

使用该商业秘密。

### 第九条 法律责任

1. 鉴于甲方商业秘密被披露、使用或允许第三人使用或转让给第三人将会削弱甲方竞争优势、造成不可估量的经济损失，为有效保护甲方商业秘密，双方约定：若乙方违反本合同规定的，赔偿金额包括但不限于因乙方侵权、违约行为给甲方造成的全部直接或间接损失，还包括甲方因乙方违约泄露、使用的商业秘密而付出的成本等实际费用。甲方遭受的损失难以计算时，赔偿额为乙方因侵权、违约行为所获取的所有经济利益。

2. 因乙方违约而导致甲方为维权而支付的合理费用，包括但不限于律师费、差旅费、人工费等，由乙方承担。

### 第十条 通知与送达

甲方可通过下列方式之一向乙方进行通知或送达：

1. 地址：\_\_\_\_\_
2. 手机：\_\_\_\_\_
3. 微信：\_\_\_\_\_
4. 电子邮箱：\_\_\_\_\_

无论乙方是否实际查阅或拒收，甲方通过上述方式之一向乙方发出通知时，即视为乙方已经查阅。如乙方联系方式变更，应立即书面告知甲方。

甲方的送达地址为：甲方办公场所。

上述地址作为有效司法送达地址。

### 第十一条 其他

1. 本合同成为甲、乙双方签订的劳动合同的重要组成部分；任何一方不得擅自变更或解除，以前签订的合同或涉及商业秘密保护的条款与本合同有不一致的地方，以本合同为准。

2. 本合同一式二份，甲、乙双方各执一份，自甲乙双方签章之日起生效，具有同等法律效力。

(以下无正文)

甲 方（签章）：

乙 方（签名）：

法定代表人/授权代表：

签订地点：

签订日期： 年 月 日

附 录 E  
(资料性)  
竞业限制协议(参考文本)

甲 方(用人单位): \_\_\_\_\_

统一社会信用代码: \_\_\_\_\_

住所地: \_\_\_\_\_

乙 方(劳动者): \_\_\_\_\_

身份证号码: \_\_\_\_\_

联系电话: \_\_\_\_\_

现居住地址: \_\_\_\_\_

根据《中华人民共和国民法典》《中华人民共和国劳动合同法》及相关法律法规,甲、乙双方在平等自愿的基础上,经充分友好协商,就员工竞业限制等有关事宜,达成如下协议:

1. 甲乙双方确认本协议所确定的竞业限制期间为乙方在甲方的任职期间及乙方离职后\_\_\_\_内(最长不超过劳动关系终止后两年)。乙方承诺,乙方在竞业限制期间,不得到\_\_\_\_(具体竞业限制区域)内与甲方生产或者经营同类产品、从事同类业务或有其他竞争关系的用人单位任职或提供任何服务(包括有偿及无偿)、拥有股份或利益、接受服务或获取利益;不得自行或与任何第三人合作,参与生产、经营与甲方有竞争关系的同类产品或业务。

2. 乙方承诺,甲方的客户信息、研发资料等商业秘密不受竞业限制期间的限制,乙方仍长期负有保密义务;乙方离职后,不得将甲方以前的客户介绍给与甲方有竞争关系的第三人或将与甲方有竞争关系的第三人介绍给甲方以前的客户。

3. 乙方应当配合甲方的监督与检查,如甲方提出要求,乙方应当在 7 日内向甲方提交下列证明材料,以证明自己是否履行了竞业限制协议约定的义务:

(1) 从甲方离职后,与新的单位签订的劳动合同及新的单位出具的从业证明(从业证明中应包括该单位与乙方建立劳动关系的时间、劳动合同的期限、岗位等内容),或者能够证明与新的单位存在劳动关系的其他证据;

(2) 新的单位为乙方缴纳社会保险、住房公积金的证明以及该单位知悉乙方负有竞业禁止义务的说

明；

(3) 或当乙方为自由职业或无业状态，无法提供上述(1)、(2)项证明时，可由其所在街道办事处、居委会(村委会)或有关政府部门出具的关于乙方的从业情况的证明。

乙方无论任何原因离开甲方，乙方同意甲方向其新雇主发出通知或于离职证明中注明竞业限制事项，以告知新雇主乙方之竞业限制义务。

4. 在乙方竞业限制期间即与甲方劳动关系解除或终止后\_\_\_内，甲方每月向乙方按其离职前12个月平均工资的30%支付经济补偿，具体标准为\_\_\_元/月，在乙方离职后按月打入乙方账户。乙方银行账户如下：

开户名称：\_\_\_\_\_

银行账号：\_\_\_\_\_

开户行：\_\_\_\_\_

如乙方账户有变动的，则应书面告知甲方，否则由乙方承担相应责任。

5. 乙方如违反竞业限制义务，乙方应当支付甲方违约金\_\_\_元。违约金不足以弥补甲方损失的，乙方应赔偿甲方所有的实际损失及合理费用。合理费用包括但不限于律师费、差旅费、保全费、诉讼费、鉴定费、人工费等。

如乙方的违约行为发生于在甲方任职期间，则甲方有权不经提前告知立即解除与乙方的聘用关系，并依法追究其法律责任，包括不限于违约责任与赔偿责任。

6、离职后，乙方同意甲方通过下列方式之一向乙方进行通知或送达：

(1) 地址：\_\_\_\_\_

(2) 手机：\_\_\_\_\_

(3) 微信：\_\_\_\_\_

(4) 电子邮箱：\_\_\_\_\_

无论乙方是否实际查阅或拒收，甲方通过上述方式之一向乙方发出通知时，即视为乙方已经查阅。如乙方联系方式变更，应立即书面告知甲方。

甲方的送达地址为：甲方办公场所。

上述地址作为有效司法送达地址。

7、本协议自双方签字或盖章之日起生效。

8、本协议一式两份，甲、乙双方各执一份，具有同等法律效力。

(以下无正文)



甲 方（签章）：

法定代表人/授权代表：

**重要提示：**本人已经仔细阅读上述协议，特别是其中的竞业限制义务、违约责任及违约金条款，并同意履行上述协议。

乙 方（签名）：

签署时间：        年    月    日

附 录 F  
(资料性)  
商务合作保密协议 (参考文本)

甲 方：\_\_\_\_\_

法定代表人：\_\_\_\_\_ 统一社会信用代码：\_\_\_\_\_

电 话：\_\_\_\_\_ 传 真：\_\_\_\_\_

地 址：\_\_\_\_\_

项目联系人及联系方式：\_\_\_\_\_

乙 方：\_\_\_\_\_

法定代表人：\_\_\_\_\_ 统一社会信用代码：\_\_\_\_\_

电 话：\_\_\_\_\_ 传 真：\_\_\_\_\_

地 址：\_\_\_\_\_

项目联系人及联系方式：\_\_\_\_\_

甲乙双方正在就\_\_\_\_\_事项进行商务合作，双方在谈判或合作期间，均因合作需要可能接触或掌握对方有价值的保密信息（包括但不限于口头、书面或其他任何形式），双方本着平等自愿、协商一致、诚实守信的原则，为保护双方商业秘密事宜，签署本保密协议以共同执行：

**第一条 术语定义**

本协议所称保密信息，企业在生产经营过程中形成的不为公众所知悉，具有商业价值并经权利人采取相应保密措施的技术信息和经营信息等商业信息。

**第二条 保密信息的范围**

经双方确认，双方在谈判或合作履约期间，因合作需要可能接触或掌握对方有价值的保密信息，包

括但不限于以下内容：

1. 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技术信息；
2. 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、数据等经营信息。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；
3. 其他符合商业秘密构成要件的商业信息。

### **第三条 双方权利义务**

1. 未经一方书面同意，另一方（包括各自代表、员工）不得向第三方（包括新闻媒体或其从业人员）公开和披露任何保密信息，或以其他方式使用保密信息。
2. 如谈判、合作项目不再继续进行，或相关合同解除、终止，一方有权在任何时候向另一方提出返还、销毁保密信息的书面要求，另一方应按要求在\_\_\_个工作日内向对方返还、销毁其占有的或控制的全部保密信息，包括但不限于保密信息的全部文件和其他材料，并保证不留有任何复制版本。
3. 甲乙双方应以不低于其对己方拥有的类似资料的保密程度来对待对方向其披露的保密信息，但在任何情况下，对保密信息的保护都不能低于合理程度。

### **第四条 保密义务期限**

甲乙双方互为保密信息的提供方和接受方，负有保密义务。本协议的义务长期有效，除非商业秘密为公众所知悉或完全公开。双方可以根据商业秘密的性质和特点，合理确定保密期限，具体保密期限为本协议签订之日起至双方终止谈判或合作后\_\_\_年止。

### **第五条 知识产权**

任何一方向另一方或其代表披露保密信息，并不代表同意另一方任意使用其商业秘密、商标、专利、著作权及其他知识产权。

### **第六条 违约责任**

1. 任何一方如违反本协议下的保密义务，应承担违约责任。双方约定，本协议项下之违约金（以下简称“违约金”），其违约金数额相当于双方拟达成或已达成合作金额的\_\_\_%。如本条款约定的上述违

约金不足以弥补因违反保密义务而给受害方造成的损失，受害方有权进一步向侵权、违约方主张损失赔偿。

2. 在双方谈判或合作期间内，无论上述违约金给付与否，受害方均有权立即终止谈判或解除与违约方的合同、合作关系，因终止谈判或解除合同、合作所造成的缔约过失赔偿责任、合同赔偿损失由违约方自行承担。

3. 损失赔偿的范围包括但不限于以下费用：

(1) 受害方为处理此次纠纷支付的费用，包括但不限于律师费、诉讼费、差旅费、材料费、调查费、评估费、鉴定费等；

(2) 受害方因此而遭受商业利益的损失，包括但不限于可得利益的损失、技术开发转让费用的损失等。

4. 在保密期间内，任何一方对本协议任何一项的违约，都会给另一方带来不能弥补的损害，并且具有持续性，难以或不可能完全以金钱计算出受损程度，因此除按法律规定和本协议约定执行任何有关损害赔偿责任外，任何一方均有权采取合理的方式来减轻损失，包括但不限于指定措施和限制使用的合理请求。

### **第七条 适用法律和争议解决**

因执行本合同而发生纠纷，可以由双方协商解决或者共同委托双方信任的第三方调解。协商、调解不成或者一方不愿意协商、调解的，任何一方都可向甲方所在地仲裁委员会提起仲裁。

### **第八条 通知与送达**

双方当事人就履行本协议过程中涉及各类通知以及就本协议发生纠纷时法院、仲裁机构的法律文书送达作出如下约定：

1. 甲方确认其有效的送达地址为：\_\_\_\_\_，授权联系人姓名\_\_\_\_\_电话：\_\_\_\_\_，电子邮箱地址：\_\_\_\_\_。

2. 乙方确认其有效的送达地址为：\_\_\_\_\_，授权联系人姓名\_\_\_\_\_电话：\_\_\_\_\_，电子邮箱地址：\_\_\_\_\_。

3. 上述地址作为有效司法送达地址。任何一方上述联系方式发生变更的，变更方应及时书面通知对方。

4. 本通知送达条款具有独立效力，不因合同整体或部分条款无效而无效。

### 第九条 其他

1. 本协议自甲乙双方法定代表人或授权代表签字盖章之日起生效，且未经双方书面协议不得补充或修改。本协议签署、履行、解释和争议解决均适用中华人民共和国法律。

2. 本协议一式\_\_\_\_份，双方各执\_\_\_\_份，具有同等法律效力。

（以下无正文）

甲 方（盖章）：

乙 方（盖章）：

法定代表人/授权代表：

法定代表人/授权代表：

日 期：

日 期：

签订地点：

**附录 G**  
**(资料性)**  
**重点行业商业秘密保护要点**

**G.1 数字经济业**

**G.1.1 技术和开发**

技术和开发的商业秘密保护要点包括但不限于算法和代码、技术架构，具体如下：

- a) 算法和代码：用于数据分析、机器学习、人工智能等的专有算法和源代码；
- b) 软件和工具：自研或独家使用的软件、工具或平台；
- c) 技术架构：企业应当重点保护数据系统的设计和架构，包括硬件和软件的整合。

**G.1.2 数据**

数据的商业秘密保护要点包括但不限于用户数据、商务数据、数据集、市场研究数据，具体如下：

- a) 用户数据：指用户的个人信息、购买历史、行为数据等；
- b) 商务数据：指销售、供应链、库存、财务等企业运营数据。
- c) 数据集：指用于机器学习和 AI 训练的专有数据集；
- d) 市场研究数据：指对竞争对手的分析、市场趋势的分析、消费者行为的分析产生的数据。

**G.1.3 网络安全**

网络安全的商业秘密保护要点包括但不限于安全策略和协议、安全漏洞和修复，具体如下：

- a) 安全策略和协议：指用于保护数据和系统的安全策略、工具和实践；
- b) 安全漏洞和修复：指对已知但未公开的系统安全漏洞及其修复方法。

**G.1.4 运营和管理**

运营和管理的商业秘密保护要点包括但不限于内部流程、人员信息，具体如下：

- a) 内部流程：指数字化的内部操作和管理流程、工具和策略；
- b) 人员信息：指关键人员、团队的技能、经验和职责等信息。

**G.2 现代金融业**

**G.2.1 技术和算法**

技术和算法的商业秘密保护要点包括但不限于定价模型、风险评估模型、交易算法、数据分析工具，具体如下：

- a) 定价模型：用于金融产品定价的算法和模型；
- b) 风险评估模型：用于评估信贷、投资等风险的专有模型；
- c) 交易算法：高频交易、算法交易的策略和代码；
- d) 数据分析工具：用于市场研究、客户行为分析等的工具和软件。

**G.2.2 数据**

数据的商业秘密保护要点包括但不限于客户数据、市场数据、交易数据，具体如下：

- a) 客户数据：客户的个人信息、财务状况、交易历史、信用记录等；
- b) 市场数据：未公开的市场调查、趋势分析、竞争对手数据等；
- c) 交易数据：交易量、交易时间、交易价格等详细交易记录。

### G.2.3 商业策略和产品

商业策略和产品的商业秘密保护要点包括但不限于新产品策略、市场入口和退出策略、投资策略，具体如下：

- a) 新产品策略：即将推出的金融产品或服务的详细信息；
- b) 市场入口和退出策略：针对特定市场或投资的策略；
- c) 投资策略：对特定资产类别、地域或行业的投资策略。

### G.2.4 合作和合同

合作和合同的商业秘密保护要点包括但不限于合作协议、投资和并购，具体如下：

- a) 合作协议：与其他金融机构、技术供应商或其他第三方的合作细节；
- b) 投资和并购：关于并购目标、价格、策略的信息。

### G.2.5 运营和管理

运营和管理的商业秘密保护要点包括但不限于内部流程、员工信息，具体如下：

- a) 内部流程：如风险管理、合规、审计、客户服务的内部流程和策略；
- b) 员工信息：尤其是高级管理和关键岗位员工的技能、经验、职责等。

### G.2.6 网络安全与技术

网络安全与技术的商业秘密保护要点包括但不限于安全协议和措施、技术架构，具体如下：

- a) 安全协议和措施：用于保护金融数据和系统的安全策略和工具；
- b) 技术架构：金融系统的设计、架构和实施细节。

### G.2.7 其他

其他的商业秘密保护要点包括但不限于研发项目。如正在进行但尚未公开的金融技术研发项目和创新。

## G.3 先进制造业

### G.3.1 技术与研发

技术与研发的商业秘密保护要点包括但不限于生产技术、研发资料、设计文件，具体如下：

- a) 生产技术：如新型的加工方法、合成路径或自动化技术；
- b) 研发资料：正在进行的研究、开发和测试的详细资料和结果；
- c) 设计文件：产品的设计图纸、3D模型、电路图。

### G.3.2 工艺与方法

工艺与方法的商业秘密保护要点包括但不限于生产工艺、质量控制标准、供应链管理方法，具体如下：

- a) 生产工艺：如特定的加工步骤、参数设置和质量控制手段；
- b) 质量控制标准：专有的检测、测试和评估方法；

- c) 供应链管理方法：如库存控制、物流优化的专有方法。

### G.3.3 机器与设备

机器与设备的商业秘密保护要点包括但不限于自研设备、设备配置与参数，具体如下：

- a) 自研设备：为满足特定需求而自行研发的生产设备或工具；
- b) 设备配置与参数：特定设备的配置、操作参数和优化设置。

### G.3.4 材料

材料的商业秘密保护要点包括但不限于专有材料、材料处理方法，具体如下：

- a) 专有材料：自行开发或独家采购的原材料、合成材料或半成品；
- b) 材料处理方法：如材料的预处理、后处理或改性方法。

### G.3.5 软件与自动化

软件与自动化的商业秘密保护要点包括但不限于生产控制软件、机器人技术，具体如下：

- a) 生产控制软件：用于生产线控制、监控和优化的专有软件；
- b) 机器人技术：机器人的编程、控制和应用技巧。

### G.3.6 数据与分析

数据与分析的商业秘密保护要点包括但不限于生产数据、数据分析方法，具体如下：

- a) 生产数据：生产过程中收集的数据，如生产速度、质量指标、设备状态等；
- b) 数据分析方法：用于生产优化、预测维护、产品质量分析的方法和工具。

### G.3.7 人员与培训

人员与培训的商业秘密保护要点包括但不限于专家知识、培训资料，具体如下：

- a) 专家知识：关键人员、工程师或研究员的专有知识、技能和经验；
- b) 培训资料：用于员工培训的专有材料和方法。

### G.3.8 商务信息

商务信息的商业秘密保护要点包括但不限于供应商与客户信息、价格策略，具体如下：

- a) 供应商与客户信息：特定的供应商或客户信息、合同和协议；
- b) 价格策略：产品的定价、折扣、促销策略等。

## G.4 商务服务业

### G.4.1 方法与策略

方法与策略的商业秘密保护要点包括但不限于咨询方法、市场研究技巧、培训方法，具体如下：

- a) 咨询方法：为特定问题或行业开发的独特解决方案和策略；
- b) 市场研究技巧：专有的市场调查、数据分析或预测方法；
- c) 培训方法：独特的培训课程、资料和方法。

### G.4.2 数据与分析

数据与分析的商业秘密保护要点包括但不限于客户数据、市场数据、项目报告，具体如下：

- a) 客户数据：客户的业务信息、需求、偏好和反馈；



- b) 市场数据：包括行业趋势、竞争对手信息、消费者行为等；
- c) 项目报告：为客户完成的咨询、研究或分析报告。

#### G.4.3 技术与工具

技术与工具的商业秘密保护要点包括但不限于软件工具、分析模型，具体如下：

- a) 软件工具：自主开发或独家使用的业务分析、管理或咨询软件；
- b) 分析模型：如金融模型、风险评估模型等。

#### G.4.4 合同与协议

合同与协议的商业秘密保护要点包括但不限于客户合同、供应商和合作伙伴关系，具体如下：

- a) 客户合同：与客户的商务条款、价格和服务细节；
- b) 供应商和合作伙伴关系：独家供应、合作或外包协议。

#### G.4.5 人员与关系

人员与关系的商业秘密保护要点包括但不限于人才信息、人脉关系，具体如下：

- a) 人才信息：关键员工、咨询师或专家的技能、经验和专长；
- b) 人脉关系：与特定行业、机构、人员建立的特定关系。

#### G.4.6 运营与管理

运营与管理的商业秘密保护要点包括但不限于内部流程、价格策略，具体如下：

- a) 内部流程：包括项目管理、客户服务、质量控制的方法和标准；
- b) 价格策略：服务定价、折扣和促销策略。

### G.5 文化旅游业

#### G.5.1 创意和内容

创意和内容的商业秘密保护要点包括但不限于初步创意和概念、手稿和原稿、研发材料、未公开的艺术作品，具体如下：

- a) 初步创意和概念：如一个新项目、产品或服务的原始构思；
- b) 手稿和原稿：如脚本、故事板、歌词、小说、设计图等；
- c) 研发材料：对于新项目、作品或技术的研究、试验和开发资料；
- d) 未公开的艺术作品：如绘画、雕塑、摄影、设计作品等。

#### G.5.2 技术和工艺

技术和工艺的商业秘密保护要点包括但不限于制作技术、独特的手工艺技术、技术软件和工具，具体如下：

- a) 制作技术：如动画制作、特效技术、录音技术等；
- b) 独特的手工艺技术：手工制品的制作方法、工艺等；
- c) 技术软件和工具：自研或独有的软件、工具或技术解决方案。

#### G.5.3 策略与计划

策略与计划的商业秘密保护要点包括但不限于营销策略、特色活动与节目，具体如下：

- a) 营销策略：即将实施的广告、推广或合作策略；

- b) 特色活动与节目：为吸引游客而设计的独特文化体验或表演。

#### G.5.4 数据与研究

数据与研究的商业秘密保护要点包括但不限于客户数据、市场研究、内部调查与报告，具体如下：

- a) 客户数据：包括顾客的偏好、消费习惯和反馈；
- b) 市场研究：对特定目的地、文化活动或旅游产品的市场调查和分析；
- c) 内部调查与报告：对服务质量、游客满意度等方面的内部研究。

#### G.5.5 技术与工具

技术与工具的商业秘密保护要点包括但不限于预订系统、虚拟现实或增强现实技术、移动应用，具体如下：

- a) 预订系统：自主开发的或独家使用的预订和管理系统；
- b) 虚拟现实或增强现实技术：用于增强文化体验或旅游导览的技术；
- c) 移动应用：为客户提供信息、导航和其他服务的专有应用程序。

#### G.5.6 合作与合同

合作与合同的商业秘密保护要点包括但不限于独家合作、供应商合同，具体如下：

- a) 独家合作：与特定文化机构、艺术家或表演团队的独家合作协议；
- b) 供应商合同：与酒店、餐厅、交通提供者等的特殊合同和条款。

### G.6 食品加工业

#### G.6.1 配方与原料

配方与原料的商业秘密保护要点包括但不限于独特配方、原料来源，具体如下：

- a) 独特配方：用于生产特定产品的独特食品配方；
- b) 原料来源：特定原料的供应商、种植或养殖技术。

#### G.6.2 生产与加工技术

生产与加工技术的商业秘密保护要点包括但不限于加工方法、设备设置、质量控制流程，具体如下：

- a) 加工方法：如某种特定的烹饪、发酵或制冷技术；
- b) 设备设置：特定机器的操作参数或设置；
- c) 质量控制流程：确保产品一致性和品质的内部测试和控制流程。

#### G.6.3 供应链与物流

供应链与物流的商业秘密保护要点包括但不限于供应商协议、物流策略，具体如下：

- a) 供应商协议：与关键供应商的独家协议或优惠条款；
- b) 物流策略：保持产品新鲜或安全的特定物流和存储方法。

#### G.6.4 市场与销售

市场与销售的商业秘密保护要点包括但不限于营销策略、客户名单，具体如下：

- a) 营销策略：即将推出的广告或推广活动、未公开的市场研究数据；
- b) 客户名单：大客户或长期合作伙伴的信息。

#### G.6.5 研发与创新

研发与创新的商业秘密保护要点包括但不限于研发项目、实验数据，具体如下：

- a) 研发项目：正在进行的或计划中的研发项目；
- b) 实验数据：新产品或技术的实验和测试数据。

#### G. 6.6 合作与合同

合作与合同的商业秘密保护要点包括但不限于合作协议、许可与分销，具体如下：

- a) 合作协议：与研究机构、大学或其他公司的研发或商务合作协议；
- b) 许可与分销：独家分销或许可的细节和条款。

#### G. 6.7 企业管理

企业管理的商业秘密保护要点包括但不限于企业策略、财务信息，具体如下：

- a) 企业策略：如未来的扩张、收购或投资计划；
- b) 财务信息：如利润率、成本结构和财务预测。

#### G. 6.8 食品安全与规范

食品安全与规范的商业秘密保护要点包括但不限于内部标准、食品安全数据，具体如下：

- a) 内部标准：超出法律要求的公司内部食品安全和质量标准；
- b) 食品安全数据：关于产品安全性的内部测试和研究数据。

### G. 7 生物医药业

#### G. 7.1 研究与开发

研究与开发的商业秘密保护要点包括但不限于药物配方、生物技术、临床试验数据，具体如下：

- a) 药物配方：新药或生物制品的独特配方或组成；
- b) 生物技术：如基因编辑技术、细胞治疗技术、蛋白质工程技术等；
- c) 临床试验数据：未公开的临床试验结果、实验数据、研究方法和研究结论。

#### G. 7.2 生产技术

生产技术的商业秘密保护要点包括但不限于制造流程、纯化与提取方法、质量控制标准，具体如下：

- a) 制造流程：生物药物或药物的生产流程、生物反应器的运行参数等；
- b) 纯化与提取方法：从生物物质中提取和纯化有效成分的技术；
- c) 质量控制标准：内部的药物质量和安全标准、检测技术和方法。

#### G. 7.3 商务信息

商务信息的商业秘密保护要点包括但不限于市场策略、供应链信息，具体如下：

- a) 市场策略：市场进入、推广、定价策略或未来市场发展计划；
- b) 供应链信息：关于原材料供应商、价格、合同细节的信息。

#### G. 7.4 合作与合同

合作与合同的商业秘密保护要点包括但不限于研发合作、临床试验协议，具体如下：

- a) 研发合作：与其他公司、研究机构或大学的合作研究协议；
- b) 临床试验协议：与医院或其他研究机构的临床试验合作协议。

#### G. 7.5 技术与软件

技术与软件的商业秘密保护要点包括但不限于研发工具、生产管理系统，具体如下：

- a) 研发工具：用于研发的专有软件、数据库或实验技术；
- b) 生产管理系统：用于生产、质量控制或供应链管理的专有软件或系统。

#### G. 7. 6 人员与培训

人员培训的商业秘密保护要点包括但不限于专家知识、培训资料，具体如下：

- a) 专家知识：员工或研究者的独特技能、知识和经验；
- b) 培训资料：关于新技术、新方法或新产品的内部培训资料。

#### G. 7. 7 其他

其他的商业秘密保护要点包括但不限于投资与并购信息、法规与合规信息，具体如下：

- a) 投资与并购信息：与潜在投资或并购目标的谈判和评估信息；
  - b) 法规与合规信息：内部的法规合规策略、监管沟通记录等。
-