北京市海淀区互联网企业商业秘密保护

工作指南

（征求意见稿）

目录

[1. 实施目的 3](#_Toc150171429)

[2. 实施范围 3](#_Toc150171430)

[3. 术语和定义 3](#_Toc150171431)

[3.1 互联网企业 3](#_Toc150171432)

[3.2 商业秘密 3](#_Toc150171433)

[3.3 秘密点 3](#_Toc150171434)

[3.4 涉密载体 3](#_Toc150171435)

[3.5 涉密区域 3](#_Toc150171436)

[3.6 数据 4](#_Toc150171437)

[3.7 算法 4](#_Toc150171438)

[3.8 代码 4](#_Toc150171439)

[3.9 模型 4](#_Toc150171440)

[4.基本原则 4](#_Toc150171441)

[4.1 企业自主 4](#_Toc150171442)

[4.2 预防为先 4](#_Toc150171443)

[4.3 多元协同 4](#_Toc150171444)

[4.4 依法维权 4](#_Toc150171445)

[4.5 公益保护 4](#_Toc150171446)

[5.总体要求 5](#_Toc150171447)

[5.1商业秘密管理体系 5](#_Toc150171448)

[5.2商业秘密管理制度 5](#_Toc150171449)

[5.3商业秘密审查 5](#_Toc150171450)

[5.4数据保护总体要求 5](#_Toc150171451)

[5.5.算法保护总体要求 5](#_Toc150171452)

[6. 商业秘密的确定 6](#_Toc150171453)

[6.1 商业秘密的范围确定 6](#_Toc150171454)

[6.2 商业秘密的构成条件 6](#_Toc150171455)

[6.3 解密 7](#_Toc150171456)

[6.4 数据、算法商业秘密的确定 7](#_Toc150171457)

[7. 商业秘密的存储 7](#_Toc150171458)

[7.1 存储载体 7](#_Toc150171459)

[7.2 商业秘密的备份 8](#_Toc150171460)

[7.3 秘密载体的封存 8](#_Toc150171461)

[7.4 商业秘密的销毁 8](#_Toc150171462)

[8. 商业秘密的分级管理 8](#_Toc150171463)

[8.1 商业秘密分级 8](#_Toc150171464)

[8.2 企业人员权限划分 9](#_Toc150171465)

[8.3 商业秘密的流转 9](#_Toc150171466)

[9. 商业秘密的保密措施 10](#_Toc150171467)

[9.1 涉密管理 10](#_Toc150171468)

[9.2 加注标记 11](#_Toc150171469)

[9.3 技术措施 11](#_Toc150171470)

[9.4 保密协议 12](#_Toc150171471)

[9.5 算法商业秘密保密措施 12](#_Toc150171472)

[9.6 数据商业秘密保密措施 1](#_Toc150171473)3

[10. 商业秘密的侵权 15](#_Toc150171474)

[10.1 侵权行为类型 15](#_Toc150171475)

[10.2 侵权行为的举证 15](#_Toc150171476)

[10.3 不属于侵犯商业秘密的情形 17](#_Toc150171477)

[11. 商业秘密侵权的维权措施 17](#_Toc150171478)

[11.1 协商和解 17](#_Toc150171479)

[11.2 人民调解 17](#_Toc150171480)

[11.3 行政保护 17](#_Toc150171481)

[11.4 申请仲裁 17](#_Toc150171482)

[11.5 司法保护 17](#_Toc150171483)

[12. 商业秘密泄密的预防 18](#_Toc150171484)

[12.1 保密教育 18](#_Toc150171485)

[12.2 日常演练 18](#_Toc150171486)

[12.3 检查监督 18](#_Toc150171487)

[12.4 日常管理 18](#_Toc150171488)

[13.应急措施 18](#_Toc150171489)

[13.1 应急预案 18](#_Toc150171490)

[13.2 定级处理 18](#_Toc150171491)

[13.3 处理程序 19](#_Toc150171492)

**1. 实施目的**

信息及互联网产业是海淀区的首位产业，信息产业中互联网企业的各类技术信息、经营信息密集，商业秘密保护需求较为强烈。本指南旨在引导本区互联网企业依据现有法律法规和自身发展战略方向，确定商业秘密保护范围，建立完善商业秘密管理体系，预防商业秘密侵权风险，营造互联网行业重视商业秘密利用与保护的良好氛围。

**2. 实施范围**

本指南规定了商业秘密保护的术语和定义、基本原则、商业秘密的确定、固定、分级管理、常见保密措施、侵权情形、维权措施及商业秘密泄露的预防。

本指南主要适用于以下互联网企业，作为相关企业开展商业秘密保护工作的工作框架及参考指南：

（1）需要建立完善企业内部商业秘密管理体系，降低商业秘密泄露风险的企业；

（2）具有商业秘密被侵害风险，积极采取商业秘密保护措施的企业；

（3）面临商业秘密纠纷，需要确定侵权行为及采取维权措施的企业；

（4）具有商业秘密保护需求的其他非互联网领域企业可参照本指南进行。

**3. 术语和定义**

**3.1 互联网企业**

互联网企业是指以互联网技术为主要生产方式，主要业务是开发互联网产品，提供互联网服务，通过互联网渠道获得主营业务收入的企业，包括基础层互联网企业、服务层互联网企业、终端层互联网企业。

**3.2 商业秘密**

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、经营信息等商业信息。

**3.3 秘密点**

秘密点，即指商业秘密的权利范围。技术秘密案件的秘密点，是指区别于公

知信息的具体技术方案或技术信息；经营信息案件的秘密点，是指区别于公知信息的特殊客户信息等经营信息。

**3.4涉密载体**

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介质。包括纸质资料、存储设备和其他承载信息的载体。

**3.5 涉密区域**

含有商业秘密信息，人员进入或访问后可能接触到商业秘密的物理区域或网络区域。

**3.6 数据**

数据，是指任何以电子或者其他方式对信息的记录。互联网企业数据主要含各类业务运营数据、用户数据和员工数据、应用系统存储产生的数据等。

**3.7 算法**

算法指解题方案的准确而完整的描述，是一系列解决问题的清晰指令，代表着用系统的方法描述[解决问题的策略](https://baike.baidu.com/item/%E8%A7%A3%E5%86%B3%E9%97%AE%E9%A2%98%E7%9A%84%E7%AD%96%E7%95%A5/56095568?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E7%AE%97%E6%B3%95/_blank)机制，包括生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等算法技术。

**3.8 代码**

代码指程序员用[开发工具](https://baike.baidu.com/item/%E5%BC%80%E5%8F%91%E5%B7%A5%E5%85%B7/10464557?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/_blank)所支持的语言写出来的[源文件](https://baike.baidu.com/item/%E6%BA%90%E6%96%87%E4%BB%B6/6999107?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/_blank)，是一组由[字符](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6/4768913?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/_blank)、符号或信号[码元](https://baike.baidu.com/item/%E7%A0%81%E5%85%83/10525003?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/_blank)以离散形式表示信息的明确的规则体系。

**3.9 模型**

模型指人工智能算法在数据上进行训练后的产物。

**4.基本原则**

**4.1 企业自主**

充分发挥企业自主性，参照本指南给出的工作框架，结合企业自身情况，设立商业秘密保护部门或依托法务或合规等相关部门开展商业秘密保护工作，制定相应的商业秘密管理制度，预防商业秘密泄露风险；在商业秘密侵权行为发生后及时采取应急措施，积极维权。

**4.2 预防为先**

增强商业秘密保护的意识和能力，建立企业商业秘密保护体系，做好商业秘密的确定、固定、分级管理工作，加强保密事项的管理，最大限度预防商业秘密泄露或侵权行为发生，在企业内部开展保密宣传，营造商业秘密保护氛围。

**4.3 多元协同**

发挥行政部门、企业、社会第三方服务机构等多方力量进行宣传培训、技术咨询、制度建设等服务，提升行业整体商业秘密保护能力。

**4.4 依法维权**

企业应依法开展商业秘密保护工作。依据现有法律法规对本企业商业秘密采取保护措施，商业秘密受到侵害时，向行政管理机构、公安机关及司法机关等寻求保护，维护合法权益。

**4.5 公益保护**

商业秘密的保护不得损害社会公共利益和他人的合法权益。损害国家利益或危及国家安全、损害公共利益和公众健康、违背公序良俗和伦理道德、危害自然环境或社会安全的信息不得作为商业秘密保护。

**5.总体要求**

**5.1商业秘密管理体系**

企业应构建完善的商业秘密管理体系。应在企业内部设置商业秘密管理职责部门，搭建商业秘密保护组织机构，总体负责企业商业秘密管理各项工作；并在各部门设置商业秘密管理人员或管理小组，在商业秘密管理部门的领导下开展本部门商业秘密管理各项工作。

**5.2商业秘密管理制度**

企业应根据自身情况，制定适用于细分领域的商业秘密管理制度，提升商业秘密管理工作的规范性，内容可包括：

a) 企业商业秘密管理体系；

b) 商业秘密的确定与分级；

c) 涉密人员管理机制；

d) 涉密物品管理机制；

e) 涉密区域管理机制；

f) 员工保密事项规定；

g) 泄密预警和应急处置机制；

h)商业秘密对外披露机制；

i) 奖惩管理。

**5.3商业秘密审查**

企业应定期或不定期组织开展商业秘密审查工作，包括：

a)对常见各项商业秘密情况进行审查，编制和更新商业秘密清单或台账，商业秘密清单可包括秘密主题、保密等级、保密期限、主责部门、保密范围、存储方式等；

b)对涉密载体和涉密区域进行检查；

c)开展商业秘密宣传教育工作；

d)对商业秘密管理体系进行评估与改进；

e）对涉密人员的管理机制、执行情况、人员变动等进行检查和评估。

**5.4 数据保护总体要求**

5.4.1 商业秘密保护应贯穿数据的全生命周期，包括数据的采集环节、存储环节、处理环节、传输环节、销毁环节等各环节。

5.4.2 企业进行数据保护时应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

5.5.算法保护总体要求

5.5.1 商业秘密保护应贯穿算法开发利用的全流程，包括算法设计、算法学习及算法应用等过程，在研发过程中注意各环节保密协议的签署存档。

5.5.2 企业进行算法保护不得损害公共利益和他人的合法权利，不得违反法律法规对于公开或公示相关算法信息的要求。

5.5.3 企业应注重利用技术手段对人工智能技术进行商业秘密保护，保护应以其使用的模型、prompt等自然语言处理技术为重点。

**6. 商业秘密的确定**

**6.1 商业秘密的范围确定**

6.1.1商业秘密中的技术信息包括：

a)设计信息：与产品或服务有关的程序、图纸、模型、产品结构、策划或设计方案、样品、样式、试验记录、技术总结报告等； 

b)；软件信息：源代码、编码、网络协议、应用程序、算法、系统底层、非公开数据、数据报告等数据加工成果等；

c)其他技术信息 

6.1.2商业秘密中的经营信息包括：

a)经营信息：经营计划、发展规划、营销计划、定价策略、商业模式、创意、管理方法、招投标材料、并购信息、运营成本、原材料资源、定价政策、合作协议等；

b)管理信息：内部管理信息、管理文件、规章制度等；

c)客户、供应商与其他合作方的信息：网络、名称、地址、联系方式以及交易习惯、交易倾向、交易模式、产品性能及交易需求、需求类型、验收标准、支付标准、支付方式、特殊经营规律、价格承受能力、利润空间、采购需求、产品成本价、产品警戒价、相关负责人性格特点等客户信息及进行整理、加工后形成的名单，以上客户包括已具有商业往来的客户及潜在客户；

d) 财务信息：财务账册、财务报表、预决算报告、审计报告、股权分配资料等；

e)人力资源信息：员工薪酬、人力资源计划、员工档案、内部组织机构、入职和离职信息等；

f)其他经营信息。

6.1.3 下列信息不应作为企业的商业秘密：

a) 公知信息和基础理论；

b) 已申请并公开的专利技术信息；

c) 公众可通过反向工程等合法途径获得的信息；

d) 法律、法规、规章及相关司法解释规定的其他情形。

**6.2 商业秘密的构成条件**

6.2.1商业秘密须符合以下条件：

a)不为公众所知悉。要求该信息不被相关领域的人所普遍知悉，“相关领域的人”指该信息同行业的从业者、竞争者或对该行业或特定范围内情况较为了解的人。

b)具备商业价值。要求该信息应能为权利人带来直接或间接的经济利益或竞争优势，包括潜在的经济利益和竞争优势；

c)权利人采取相应保密措施。包括对商业秘密本身的保护，对内部员工的保密要求，以及对外部人员的防范等。保密措施须与信息的经济价值、泄密风险相匹配。

6.2.2商业秘密确认的实施人员应依据企业行业属性、各部门流程与项目特性，定期开展各部门商业秘密确认工作，确定具体秘密点，并将各部门商业秘密进行汇总，由企业商业秘密管理部门制定企业商业秘密清单。

6.2.3如商业秘密属于国家秘密的，应按照国家秘密相关法律法规进行管理。

6.2.4企业商业秘密管理部门定期或在重大研发项目完成后组织各部门商业秘密管理人员对企业商业秘密进行清点、梳理、筛选与记录，及时更新企业商业秘密清单。

**6.3 解密**

已确定的企业商业秘密出现下列情形时，可予以解密：

a) 因技术进步等因素，企业认为商业秘密事项已不再具有保护价值的；

b) 商业秘密已被合法公开的；

c）企业自主决定不再作为商业秘密予以保护。

**6.4 数据、算法商业秘密的确定**

作为商业秘密保护的算法符合以下条件：

1. 不为公众所知悉，公共数据、开源代码和第三方已公开代码不得作为商业秘密进行保护;
2. 具有商业价值，因企业数据、算法及代码一般涉及企业核心竞争力，应作为较高等级的商业秘密进行保护。
3. 权利人采取相应保密措施，保密措施应满足能抵御物理及互联网双重风险的要求。

企业可以将算法中的相关代码、数据、序列、结构、组织、框架等要素作为密点进行具有较高可识别性的确定。

**7. 商业秘密的存储**

**7.1 存储载体**

7.1.1本地化信息系统

企业可建立信息系统进行商业秘密的存储。

7.1.2云端存储空间

企业可通过云端存储商业秘密，但应就云端存储的配置要求、存储容量、风险情况、账户权限划分等事项与云服务商进行明确约定，以确保云端存储的保密性、安全性及稳定性。

7.1.3硬件存储设备

存储设备包括移动硬盘、可记录光盘、MP3、MP4、U盘、闪存、网盘等以光学、磁性、半导体、云端存储方式进行存储的设备。

7.1.4纸质资料

商业秘密可以纸质资料形式存储，资料持有部门应做好归档保管工作。

**7.2 商业秘密的备份**

7.2.1以纸张、存储设备等物理形式存储的商业秘密，可根据商业秘密自身情况备份至企业统一管理的信息系统或云端存储空间，避免因意外情况毁损灭失。

7.2.2 当存储设备因技术进步淘汰等原因不再适宜作为存储载体时，应及时更换方式进行商业秘密存储。

**7.3 秘密载体的封存**

7.3.1 具备以下特征的涉密载体应当进行封存：

a)所存储的商业秘密名称、内容等信息不再进行变化，且将长期发挥作用；

b)可能作为商业秘密权利人的重要证据；

c)企业认为有必要进行封存的其他载体。

7.3.2 应采用可长期保存、不易遗失毁损、有信息安全保护的存储设备和方式进行涉密载体封存。

7.3.3 商业秘密管理部门应定期对封存载体进行审查，确保其内容的完整性和不可获得性，并进行持续维护。

**7.4 商业秘密的销毁**

7.4.1 涉密信息使用完毕后，使用人应在商业秘密管理部门人员的监督下将商业秘密或涉密载体销毁，商业秘密管理部门应定期组织审查商业秘密存储情况。

7.4.2 可选择采取下列方式对销毁过程进行监督管理：

a) 对销毁过程进行录像；

b) 在本部门商业秘密管理人员的监督下销毁；

7.4.3 商业秘密的销毁应达到秘密无法得以恢复的效果，如：

a) 纸质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等方式进行永久删除；

c) 其他合适的方式。

**8. 商业秘密的分级管理**

**8.1 商业秘密分级**

8.1.1企业可重点评估以下因素，科学划定商业秘密等级：

a)商业秘密可能带来的商业价值；

b)泄露后对企业造成的危害程度；

c)该信息研发开发成本、生命周期、技术成熟度、保密的可行性以及反向

工程的难易程度；

d)该信息所在行业领域的情况、周边技术情况；

e)商业秘密泄露后可能承担的法律责任；

f)商业秘密目前在企业内被知悉的范围。

其中企业发展规划、产品技术方案、原材料资源、研发成本等事关企业核心竞争力的信息需列入较高等级的商业秘密。

8.1.2商业秘密按保密程度从高到低可分为一级商密、二级商密、三级商密或其它企业根据实际情况确立的各个保密等级。对于更高等级的商业秘密应采取更加严格的保密措施。

8.1.3商业秘密分级工作应由商业秘密管理部门组织和指导各部门商业秘密管理人员或管理小组开展，应在商业秘密确定时完成分级工作并列入商业秘密清单。当商业秘密等级内容需要更新时，应及时进行变更。

**8.2 企业人员权限划分**

8.2.1 商业秘密管理部门应依据企业工作人员职位、工作需要等因素划分接触商业秘密的权限；如因具体工作需要，可临时提升或降低权限。

8.2.2 企业可通过限制员工账户访问权限、限制进入特定涉密区域、限制接触涉密物品、限制参加涉密活动等方式，实现员工权限分级管理。

8.2.3 员工工作岗位变动前，企业应及时评估并重新划分权限，要求员工上交或删除权限之外的全部涉密资料和涉密物品，并与员工签署协议，明确其不得继续使用接触的商业秘密范围。

8.2.4 员工离职时，应当主动将涉及商业秘密信息的资料、文件、企业配发的设备归还企业，按照人力资源管理要求签署离职交接文件或相关离职协议，将商业秘密及载体全部完整归还或按企业要求将相关商业秘密销毁至不可恢复状态，且承诺离职后不会侵犯企业的商业秘密。

**8.3 商业秘密的流转**

8.3.1企业应对非依权限进行商业秘密存储载体的复制、接触行为采取严格的限制措施，经由各部门商业秘密管理人员审批并报商业秘密管理部门备案后，方可进行复制或接触，同时载明复制接触内容、使用期限、使用事项、复制设备等内容，并仅限在企业指定的设备上进行使用。

8.3.2商业秘密进行网络传递应严格采取加密措施，通过企业内部局域网或加密互联网通道进行发送，严格限制接收人员、编辑权限等内容，并做好内部局域网隔离工作，企业可根据商业秘密情况，限制通过电子邮件、公共聊天软件等方式进行商业秘密的网络传递。

8.3.3涉密载体使用完毕后，商业秘密管理人员应及时进行回收或销毁，并将使用情况进行登记留存。

8.3.4如需提取商业秘密供企业外部人员使用，应出具与使用单位或个人签订的商业秘密保密协议，并督促使用单位或个人及时归还或销毁涉密载体。

**9. 商业秘密的保密措施**

**9.1 涉密管理**

**9.1.1 涉密区域**

9.1.1.1 涉密区域识别

常见涉密区域的地点或部门包括但不限于：

（a）产品研发工作区、设计实验室、信息数据中心和其他重要生产场所；

（b）涉密档案室，财务、人力资源、销售等部门办公室的涉密档案存放区域；

（c）未公开的样品存放地点；

（d）重要原材料、重要半成品等涉密物资存放区域。

9.1.1.2 涉密区域保护

 涉密重点区域实行进出登记和保密告知，应采取的保护措施包括但不限于：

（a）涉密区域划分为相对独立的空间，进出口设置涉密区域标识；

（b）进入涉密区域需经过授权，设置门禁设施，可以采取指纹、脸部、瞳孔等合法技术手段进行权限验证；

（c）涉密区域进出口处应安装视频监控设施和报警装置，非法闯入能立即告警；

（d）涉密区域内严格限制使用具有录音、摄像、拍照、信息存储等功能的设备；

（e）涉密区域应当不接入外网，与内部网络相互隔离，采取分级管控；

（f）涉密区域的网络应当搭建独立的网络基础设施，远程访问涉密区域网络应当严格进行核验权限并搭配安全验证等措施。

**9.1.2 涉密载体**

9.1.2.1 纸质资料管理

纸质商业秘密资料应明确标有“商业秘密”字样，并标注其秘密等级及保护期限。资料持有部门应建立涉密档案，并将资料储存于干燥、阴凉的区域。确保商业秘密按权限使用，做好资料查阅、复制的审批记录工作，复制件应当进行编号登记。

9.1.2.2存储设备管理

a)存放商业秘密的移动硬盘、可记录光盘、MP3、MP4、U盘、闪存等各类存储设备，应妥善保管、归档登记；

b)存储设备可以采取加密技术手段，并仅能在企业指定的工作设备上进行使用；

c)工作设备送外维修前应经商业秘密保护部门审批，并拆卸涉密存储设备；

d)若需变更涉密存储设备用途，应预先进行脱密处理。

9.1.2.3信息系统管理

a)应严格设置信息系统访问权限，定期更换系统登录密码。

b)设置系统防火墙，一级商密、二级商密等级的商业秘密应以加密方式进行存储。

c)在系统操作界面进行保密义务提示，包括在账户登录界面、账户登录后的主界面设置保密义务提醒，在设密码文档或音视频开头加注商业秘密等级等方式。

**9.2 加注标记**

**9.2.1 保密标记**

企业可以在涉密区域、涉密载体上加注保密标记。保密标记涵盖的内容为编号、保密等级、保密期限以及责任单位等。应在涉密区域、涉密载体的显著位置进行加注，物理标记应当选择不易损坏、篡改的专用标识。网络标记应当限制更改权限，同时保存网络标记的全部更新记录。

**9.2.2 警示标记**

企业可以涉密区域、涉密载体上加注警示标记，情景包括但不限于：

（a）在涉密信息提取系统的账户登录、系统操作界面等界面中，警示使用者需要遵循的保密义务；

（b）在涉密电子文档首页、页眉、页脚、页面水印等处，警示使用者需要遵循的保密义务；

（c）在涉密音（视）频开头、结尾等处，警示使用者需要遵循的保密义务；

（d）在涉密场所的入口、出口、场所内部以及涉密载体的表面等处，警示使用者需要遵循的保密义务。

**9.3 技术措施**

**9.3.1 防火墙**

企业可以搭建防火墙，通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助企业网络与外网之间构建一道相对隔绝的保护屏障，以保护企业商业秘密不受外部侵入。

**9.3.2 加密办公工具**

企业可以开发加密办公工具或购买办公工具的加密传输服务，在企业日常运营过程中使用加密办公工具进行文件传递，严禁员工采取第三方软件对涉密文件进行传输。加密办公工具类型包括集成式网络办公系统、企业邮箱以及企业网盘等。

**9.3.3 数据泄露防护系统**

企业可以采用数据泄露防护系统，在企业内部设备加装后台程序，通过身份认证和加密控制以及使用日志的统计等手段对内部数据流转进行控制，在出现数据流动异常情形时自动报告给负责的单位，便于及时对数据流动异常情形进行处理

**9.3.4 流量监测工具**

运营网络服务程序的企业可以开发流量监测工具，检测所运营的网络服务程序的实时流量情况。在发生流量异常时及时上报主管单位，对流量异常的具体原因进行筛查、修复，以防因外部网络攻击导致商业秘密泄露。

**9.4 保密协议**

企业可以与涉及商业秘密的相对方签订保密协议。企业在与相对方签订保密协议时，要对所涉商业秘密的类型、载体、涉密内容等作出明确约定。违约责任部分，企业可以明确约定一个具体的违约赔偿金额，便于对协议相对方进行警示教育以及在涉诉时进行举证。保密费用并非保密协议的当然条款。

**9.4.1 员工协议**

企业根据岗位涉密情况，与企业自身员工签订相应的保密协议明确员工应遵守的企业商业秘密保护管理规定，以及其应履行的保密义务及承担的违约责任等。

**9.4.2 商业协议**

企业在对外开展经营活动时，涉及商业秘密的，应与相关方签订商业保密协议，或在商务合同（协议）中规定涉密信息保密要求。明确规定所涉及的商业秘密内容，以及经营伙伴应当履行的保密义务以及承担的违约责任。

**9.4.3 竞业限制协议**

企业根据岗位涉密情况，与自身离职员工签订的竞业限制协议，明确涉密人员在离职后应当遵守的竞业要求，以及其应承担的保密义务及承担的违约责任。企业应当给予竞业协议的签订人员一定的经济补偿。对于高级管理人员、高级技术人员等重要岗位员工的竞业协议，建议在员工在职期间进行签订，不要只是在员工离职时签订。

**9.5算法商业秘密保密措施**

**9.5.1重视网络安全**

进行涉密代码编写传输时使用企业内部工作网络，不得接入公共网络，可部署SSL证书以确保传输安全；技术部门定期检查企业办公系统和内部网络，及时修补漏洞；采取防火墙、态势感知、蜜罐等技术手段对网络入侵行为进行监控。

**9.5.2 内部操作监控**

针对涉密内容进行访问控制及身份认证，利用堡垒机技术对员工操作进行监控并记录访问日志。

**9.5.3 保密技术设计**

可以在算法内部嵌入预期有效的保密技术设计，减少算法自动化决策所可能造成的秘密泄露。

**9.5.4 区块链技术保护**

企业可以采取区块链技术对算法进行保密，开展效率高、成本低、保密性强、可追溯的商业秘密保护工作。

**9.5.5 模型秘密保护**

利用模型进行技术研发时，可以根据数据内容采取隐私计算等方式，预防潜在商业秘密泄露风险。

**9.6 数据商业秘密保密措施**

数据的商业秘密保护需要依照涉密数据的全生命周期，采取具体的商业秘密保护措施。

**9.6.1 数据的采集环节**

数据的采集环节是指对涉密数据进行收集和获取的环节。这一过程中，数据秘密的持有人应当遵守法律法规、部门规章和规范性文件，并对涉密数据进行分级管理，明确涉密数据的涉密等级，对不同等级的涉密数据采取不同的管理措施包括但不限于：

（a）应当制定涉密数据采集程序，明确数据采集目的、规模、方式、范围、类型、存储期限、存储地点等，并对操作行为记录和审计，避免出现超范围数据收集活动；

（b）应对涉密数据采集所涉及的软硬件工具、设备、系统、平台、接口以及收集技术等，采取必要的测试、认证、鉴权等措施，并进行内部审批；

（c）应当遵循合法、正当的原则开展数据采集，不得窃取或者以其他非法方式采集数据。

**9.6.2 数据的存储环节**

数据的存储环节是指对涉密数据以数字格式进行物理存储的环节。数据秘密持有人可以采取的保护措施包括但不限于：

（a）使用密钥管理服务，对涉密数据存储统一进行密钥管理，包括密钥创建、查看、编辑、标记、启用和禁用等；

（b）禁止企业员工使用私有加密算法对涉密数据进行加密；

（c）对于不需要还原密文的场景，必须采用随机值的哈希算法进行存储，对于需要还原密文的场景，必须使用业界认可且不易被攻破的加密算法；

（d）如对涉密数据有备份要求，应制定数据备份和恢复策略，确保所有涉密数据备份文件独立加密，同时定期对涉密数据进行本地备份，备份介质场外存放；

（e）应对存储涉密数据的使用进行身份鉴别和访问控制；

（f）应对涉密数据存储介质进行安全管理，将介质存放在安全环境中，实行存储环境专人管理；

（g）应定期进行涉密数据恢复演练，确保能够及时、完整、准确地恢复数据。

**9.6.3 数据的处理环节**

数据的处理环节是指企业对涉密数据进行分类、加工、转换等处理的环节。数据秘密持有人可以在处理环节建立安全保护机制，防止处理过程中数据泄漏、不合规操作等安全风险，数据安全保护措施包括但不限于：。

（a）应对涉及数据的处理活动进行授权和验证，遵循最小化访问原则；

（b）应采用身份鉴别、数据脱敏、数据水印、访问控制等技术手段，确保数据在处理中的环境安全；

（c）应对涉密数据进行保护，未授权的情况下无法使用涉密数据。

**9.6.4 数据的传输环节**

数据的传输环节是指涉密数据在企业内部各部门间以及企业与外部的单位之间因实际需要，对涉密数据进行的流转、交互环节。数据秘密持有人可以采取一定措施，防止数据秘密在传输过程中发生泄露，包括但不限于：

（a）涉密数据通过网络传输过程中应使用商业秘密持有人认可的加密传输协议，例如使用数字签名保证涉密数据在传输过程中的一致性和不可否认性。使用的加密算法和签名技术应符合国家相关法律法规要求；

（b）商业秘密持有人内部与外部系统之间数据接口的调用应能够提供token授权、签名、时间戳超时等机制，防止接口数据被篡改或重复调用；

（c）应限制接口调用的次数和频次，防止大量访问以及大量占用资源的情况，保证系统的可用性；

（d）涉密数据接口应采用数据加密、数据校验、安全传输通道、安全传输协议等措施保证数据传输安全，必要时可采用单向隔离传输等技术手段；

（e）应实现对接口的运行情况实时监控及报警，及时发现数据传输错误或异常；

（f）向第三方商业机构提供涉密数据时，应在双方合作协议中明确数据保护的安全责任与义务，并包含数据泄密违约惩罚机制。

**9.6.5 数据的销毁环节**

数据的销毁环节是指对数据及数据的存储介质通过各种手段，使数据彻底消除且无法恢复的阶段。为保证所销毁的数据不会遭到恶意恢复导致数据秘密泄露，数据秘密持有人可以采取一定措施，包括但不限于：

（a）涉密数据的存储介质严禁二次利用，并对介质进行消磁或彻底格式化，同时使用专用工具在存储区域填入无用信息进行覆盖；

（b）对涉密数据进行删除前，由操作人员进行登记，并提交给负责人批准，所有的涉密数据清理都应记录备案；

（c）涉密数据存储介质应建立存储媒介安全销毁的规程和技术手段，存储媒介的销毁包括但不限于物理销毁、消磁设备、格式化技术等；

（d）应对涉密数据销毁过程留存日志，记录数据销毁的审批、实施过程，以及被销毁数据的具体情况；

（e）应实现存储介质物理销毁，保证在数据完全删除后再销毁存储介质，原则上不得以任何理由、任何方式对销毁数据进行恢复。

**10. 商业秘密的侵权**

商业秘密侵权行为是未经商业秘密权利人许可，直接或间接的获取、披露、使用或许可他人使用商业秘密，使得商业秘密权利人遭受损失的行为。

**10.1 侵权行为类型**

侵犯商业秘密的行为体现为下列情形：

（a）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；

（b）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

（c）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；

（d）教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密；

（e）第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条（a）款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

**10.2 侵权行为的举证**

商业秘密的权利人应当在商业秘密侵权行为发生后及时收集相应证据，以便在后续的维权措施中用以佐证商业秘密侵权行为的存在以及自身遭受的实际经济损失。

**10.2.1 权利归属证据**

用以证明商业秘密权利归属的证据，一般为商业秘密权利人持有的技术信息、经营信息等商业信息的载体等。权利归属证据形式多样，可以为物质载体、数字载体等商业秘密权利人所持有的记录商业秘密的现实凭证，例如互联网企业存放数据的存储设备，程序、服务运行过程中产生的运维、日志数据等。

**10.2.2 秘密性证据**

用以证明商业秘密不为所属领域的相关人员普遍知悉和容易获得的证据，一般为可供鉴定机构进行司法鉴定的密点。鉴定机构能够依照商业秘密权利人所提供的密点鉴定得出所涉信息具备秘密性的特征，例如与开源软件平台相区别的新型算法，未公开的样机、模型等硬件设备的参数设置等

**10.2.3 保密性证据**

用以证明商业秘密权利人针对持有的商业秘密采取了相应保密措施的证据，一般体现为商业秘密权利人采取的具体保密行为，如互联网企业内部的涉密管理制度、在涉密区域的权限限制和载体上加注标记的行为、系统鉴权的设置、系统访问权限或数据处理权限的设置、实施的后台数据传输监测与流量监测等技术措施、与员工签署的保密协议等。

**10.2.4 价值性证据**

用以证明商业秘密权利人所持有的商业秘密具有商业价值，能够通过现在或将来的使用为商业秘密权利人带来现实或潜在的经济利益与竞争优势的证据，一般体现为商业秘密权利人为获取商业秘密所投入的精力、金钱、时间等成本，商业秘密对于商业秘密权利人属于不可或缺的技术或能够为商业秘密权利人者带来潜在经济价值等证据。

**10.2.5 接触行为证据**

用以证明商业秘密侵权行为人与所涉商业秘密有直接或间接的接触，能够获取所涉商业秘密的内容的证据，一般体现为商业秘密权利人与员工之间签署的保密协议、竞业协议以及与合作对象签订的商业合同与相关保密条款。

**10.2.6 侵权行为证据**

用以证明商业秘密侵权行为人侵犯所涉商业秘密的相关证据，一般体现为商业秘密侵权行为人所采取的申请专利、制造产品等侵害商业秘密权利人权利的行为，例如使用相同的算法、数据，公开涉密的硬件参数、交易涉密的经营信息等。侵权行为中涉及的商业信息内容应当与商业秘密的内容相同或构成实质性相似。

**10.2.7 实际损失证据**

用以证明商业秘密权利人因商业秘密侵权行为所遭受的经济损失，一般体现为互联网企业研究、开发、生产和采取保密措施所投入的费用；与他人曾就商业秘密进行有偿许可使用的相关许可使用协议、费用支付凭证等证据。

**10.2.8 侵权获利证据**

用以证明商业秘密侵权人因商业秘密侵权行为所获得的经济利益，一般体现为商业秘密侵权人营收的增加、经营活动中成本的降低、在市场竞争中获得的不正当竞争优势等

**10.2.9 司法鉴定**

在发生商业秘密侵权行为后，商业秘密权利人可以向具有司法鉴定资质的机构提供所确定的商业秘密内容与侵权造成的实际损失的证据。司法鉴定机构依据商业秘密权利人所提供的材料确定侵权行为涉及的具体商业秘密密点及商业秘密权利人遭受的实际损失金额。

**10.2.10 举证责任转移**

如商业秘密权利人在举证过程中通过提交上述证据足以证明，商业秘密侵权人所使用的信息与所涉及的商业秘密内容相同或构成实质性相似，同时商业秘密权利人能够证明商业秘密侵权人有接触其商业秘密的条件，则应当由商业秘密侵权人对自己的行为不构成侵权承担举证责任，否则应当由商业秘密侵权人承担不利后果。

**10.3 不属于侵犯商业秘密的情形**

为便利人才流动，保护社会创新环境，企业应对行为是否侵犯商业秘密进行区分，在商业秘密保护范围之外的行为不构成对企业商业秘密的侵犯，如：

（a）员工在工作中掌握和积累的一般知识、经验和技能，除属于单位的商业秘密情形外，员工有自主利用的自由，自主利用其知识不属于侵犯商业秘密；

（b）客户名单作为企业商业秘密时，如名单上的客户基于对特定员工个人的信赖，自愿与该特定员工在其离职后继续进行交易，不属于侵犯商业秘密；

（c）商业秘密权利人以外的主体，对公开渠道通过合法途径取得的产品进行反向工程获得的成果进行商业化使用，不属于侵犯商业秘密。

**11. 商业秘密侵权的维权措施**

商业秘密侵权行为发生后，商业秘密权利人可以采取一定的措施以维护自身合法权利，追究商业秘密侵权人的法律责任。

**11.1 协商和解**

商业秘密权利人可以与商业秘密侵权人在自愿互谅的基础上，就已经发生的商业秘密侵权行为进行协商并达成协议，自行解决相关民事争议。协商和解可以在商业秘密权利人维权的任何阶段进行，和解协议达成后双方的民事争议视为解决完毕。但如商业秘密侵权行为已触犯刑法，刑事责任部分则无法通过协商进行和解。

**11.2 人民调解**

商业秘密权利人与商业秘密侵权人可以就侵权争议向人民调解委员会寻求帮助。人民调解委员会通过说服、疏导等方法，促使双方在平等协商基础上自愿达成调解协议，解决商业秘密侵权纠纷。

**11.3 行政保护**

商业秘密权利人在商业秘密侵权行为发生后，可以向权利人所属辖区的市场监督管理部门提出投诉举报，向市场监督管理部门提交收集到的证据，配合市场监督管理部门进行调查执法工作。

**11.4 申请仲裁**

商业秘密权利人与商业秘密侵权人可以协商一致达成仲裁协议，一同向协议选定的仲裁委员会提出仲裁申请，由仲裁委员会就商业秘密侵权行为作出裁决。裁决作出后，仲裁委员会与人民法院将不再受理就同一商业秘密侵权纠纷提出的仲裁申请或诉讼请求。

**11.5 司法保护**

商业秘密权利人在商业秘密侵权行为发生后，可以向有管辖权的人民法院提起诉讼申请；针对有进一步侵害自身权利的情况，可以向人民法院申请禁止令；针对证据存在毁损灭失风险的情形，可以向人民法院申请证据保全。商业秘密权利人也可以向人民检察院提出法律监督申请。如涉及违法犯罪行为，可以向公安机关报案，调查取证完毕后由人民检察院对商业秘密犯罪嫌疑人提起公诉。

**12. 商业秘密泄密的预防**

为防止商业秘密侵权行为的发生，商业秘密权利人可以预先采取一定的预防措施，以防商业秘密泄密情况的发生。

**12.1 保密教育**

商业秘密权利人可以组织新入职员工、重点岗位、重要涉密人员以及全体员工参加有针对性的保密教育培训，提醒员工商业秘密的覆盖范围，告知员工商业秘密泄密行为涉及的民事责任与刑事责任风险，提高员工保守商业秘密的意识。

**12.2 日常演练**

商业秘密权利人可以常态化进行商业秘密泄密应急处理演练，模拟商业秘密泄密情形发生时的应对举措，提高自身对商业秘密泄密情形发生时的处置能力，预防泄密事件发生后损失的扩大。

**12.3 检查监督**

商业秘密权利人应制定监督检查方案，定期或不定期对商业秘密保护管理制度落实情况开展监督检查，形成监督检查结论，并依照结论对自身的商业秘密保密制度进行整改优化。

**12.4 日常管理**

商业秘密权利人可以在日常经营过程中对商业秘密保护进行宣传，通过内部文件、标识、公告栏、办公软件与企业邮件等多种措施，提醒员工商业秘密泄密事件发生的具体场景，警示员工泄密行为所需承担的民事责任与刑事责任。

**13.应急措施**

**13.1 应急预案**

商业秘密权利人可以制定商业秘密泄露的应急预案，包括成立应急小组、明确泄密事件应对流程、启动泄密溯源程序、有效制止泄密的扩散。商业秘密权利人可以常态化进行商业秘密泄密应急处理演练，提高应对能力。

**13.2 定级处理**

发现商业秘密可能遭到侵权后，应对疑似遭受侵权的情况进行分析评估，根据评估结果将侵权事件进行等级划分，评估因素包括但不限于：

a)商业秘密等级；

b)商业秘密侵权的方式，如未经许可的复制、披露给第三方、公开或使用；

c)商业秘密侵权的具体范围内容，所涉及的领域；

d)商业秘密侵权对企业造成的影响；

e)侵权嫌疑人的情况。

**13.3 处理程序**

**13.3.1 侵权行为的报告**

公司员工或相关人员发生或发现商业秘密侵权事件的，应立即向本部门商业秘密管理人员或商业秘密管理部门报告，若情况紧急也可直接向公司管理层汇报，以便及时采取补救措施。涉及国家秘密被侵权的，应立即采取补救措施，并及时向当地公安机关、国家安全机关和保密行政管理部门报告。

**13.3.2 成立工作小组**

商业秘密管理部门应与相关部门协同成立应急工作小组，根据侵权事件的等级，制定侵权事件的具体补救措施，对侵权事件进行调查和提出处理意见，向公司报告侵权事件情况。

**13.3.3 应急处置**

侵权行为发生后或有发生的迹象时，企业应迅速进行处置，防止信息进一步扩散，将损害控制在最小范围内，必要时可向公安机关报告。处置事项可包括：

a)纸质资料或存储设备等载体失窃或被未经许可复制的，应做好现场保护工作，调查并确定侵权嫌疑人、侵权原因并查找泄密范围和流向，存储设备被复制的，应查询存储设备的使用情况；

b)商业秘密被上传至信息系统或与互联网连接的计算机的，应联系相关部门对泄露信息进行屏蔽或删除；

c)商业秘密管理部门应协同人事部门、法务部门、信息技术部门对侵权嫌疑人近期利用工作设备下载、使用、流传商业秘密的记录进行查找回溯，调取其签署的保密协议等相关文件。

**13.3.4 证据收集**

发现商业秘密涉嫌被侵权时，应及时收集相关证据，并做好现场保护、证据存档等工作，具体证据内容见本指南第10条。

**13.3.5 责任追究**

商业秘密侵权行为发生后，应查明侵权行为发生原因和责任人，对侵权行为人及商业秘密管理人员等相关责任人进行责任追究。