ICS 03.100.01
A 01

DB33

浙　江　省　地　方　标　准

DB33/T XXXXX—XXXX

商业秘密保护管理与服务规范

Management and service specifications for protection of trade secrets

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

浙江省市场监督管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由浙江省市场监督管理局提出并归口。

本标准起草单位：杭州市余杭区市场监督管理局、浙江蓝箭万帮标准技术有限公司、台州市市场监督管理局价监竞争分局、杭州未来科技城（海创园）管委会、浙江省律师协会、宁波商密网知识产权有限公司、同盾科技有限公司、杭州商盾企业管理咨询有限公司、浙江省方大标准信息有限公司、浙江南浔电梯科技创新公共服务中心、浙江爱旭太阳能科技有限公司、温州明发光学科技有限公司、迈得医疗工业设备股份有限公司、温州汉风机械有限公司、宁波远景汽车零部件有限公司、浙江嵊泗森兴电器制造有限公司、宁波星箭航天机械有限公司。

本标准主要起草人：张璨文、余能超、朱盛霞、王飞、夏建华、江利良、陈佳晨、沈建强、孙建明、陈霖、朱正斌、蔡亦安、孙佳恩、程行坤、许振涛、汪维佳、姚晟连、郑玲、黄健民、王烨君、潘国强、章军华、罗巧、阮立三。

商业秘密保护管理与服务规范

1 范围

本标准规定了商业秘密保护的术语和定义、一般要求、商业秘密事项管理、企业自主保护、商业秘密维权和协同保护。

本标准主要适用于企业的商业秘密保护管理，也适用于企业集聚的园区、特色小镇的管理机构和行业协会、第三方社会服务机构为企业提供的商业秘密保护服务。科研院所等其他组织的商业秘密保护亦可参照执行。

2 术语和定义

下列术语和定义适用于本文件。

2.1

商业秘密 trade secrets

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。

注：“不为公众所知悉”、“具有商业价值”和“相应保密措施”的具体内容见《中华人民共和国反不正当竞争法》及最高人民法院发布的有关司法解释。

2.2

涉密载体 secret carriers

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、存储介质（磁性介质、光盘、U盘、硬盘、服务器等）和其他介质。

2.3

涉密物品 secret items

含有商业秘密信息的设备、原材料、半成品和样品等。

3 一般要求

3.1 应坚持“企业自主、政府指导、预防为主和依法维权”的商业秘密保护管理和服务原则。

3.2 企业应设立商业秘密保护部门或依托相关部门开展商业秘密保护工作，配备专(兼)职保密员。

3.3 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部门和专(兼)职保密员。

3.4 企业的商业秘密保护部门和保密员应履行以下职责：

a) 识别和管理商业秘密事项、涉密部门、涉密人员、涉密区域；

b) 组织企业员工进行商业秘密保护培训；

c) 组织制订、实施商业秘密保护措施；

d) 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；
e) 履行商业秘密泄露的证据整理、搜集、举证、协助调查取证等工作。

3.5 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，宜在涉及商业秘密保护的重点部门配备保密员。

3.6 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。

3.7 企业的商业秘密保护工作应实行分级管理措施：
a) 对商业秘密及涉密载体实行分级管理，按层级履行使用审批手续；
b) 对涉密场所实行区域分级管理；
c) 对涉密岗位、涉密人员实行分级管理。

3.8 应对涉密信息进行严格管控，宜按涉密岗位、业务流程等细化分割涉密信息，涉密岗位按权限接触相关的涉密信息。

3.9 应在企业内部进行保密宣传（如设置画报、标语、发送短信提醒等），营造商业秘密保护氛围。

4 商业秘密事项管理

4.1 定密

4.1.1 应对企业的商业秘密进行核查和评估，其表现形式见附录 A，评估范围应包括：
a) 涉密技术信息：与科学技术有关的结构、原料、组分、配方、材料、样式、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；
b) 涉密经营信息：与经营活动有关的创意、管理、营销、财务、计划、样本、招投标材料、数据、客户信息等，以及对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息。

4.1.2 对企业的商业秘密进行核查和评估时应考虑以下因素：
a) 信息的经济价值，包括该信息产生的现在的价值，以及该领域技术革新的速度和有无替代技术等的将来的价值；
b) 对竞争企业的价值；
c) 因信息泄露等可能遭受的损失程度；
d) 信息泄露时可能承担的法律责任；
e) 法律、法规、规章及相关司法解释等规定的其他情形。

4.1.3 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。

4.1.4 宜对技术秘密进行科技查新，确认其不为公众所知悉。

4.1.5 应建立商业秘密事项目录清单，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。

4.1.6 根据商业秘密的重要性，由高到低可依次分为核心秘密、重要秘密和一般秘密三个保护等级，实行定期复评、动态调整。

4.1.7 泄露后有可能影响国家安全和利益的商业秘密，应依法定程序将其确定为国家秘密。

4.2 隐密

4.2.1 下列情形涉及商业秘密的，应对相关信息予以隐藏：

a) 与供应商、客户、合作方等的沟通和信息往来中；
b) 信息公开、发布、流转时；
c) 协助其他单位尽职调查时；
d) 其他情形。

4.2.2 配合行政机关和部门的行政检查、行政执法行动中，涉及隐秘事项检查的，企业应主动提醒执法检查人员履行保密义务。

4.2.3 可采取的隐藏方式为：

a) 隐藏或删除涉密信息；
b) 对涉密信息进行模糊化处理；
c) 其他方式。

4.3 解密

4.3.1 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) 其它特定因素导致商业秘密被公开的。

4.3.2 企业认为不需要继续保密的信息可予以解密，可采取的解密方式为：

a) 移出涉密区域；
b) 消除或变更密级标识、提示；
c) 电子文档解密；
d) 其他方式。

4.4 销毁

4.4.1 销毁涉及商业秘密的文件（含复制文件）、资料、电子信息、载体和物品，应由保密员列出销毁清单，经商业秘密保护部门审批后实施。

4.4.2 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) 对销毁过程录像等。

4.4.3 应采取合适的方式妥善销毁：

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) 其他合适的方式。

5 企业自主保护

5.1 人员管理

5.1.1 入职管理

5.1.1.1 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/协议（见附录 B）。

5.1.1.2 高级管理人员、高级技术人员及其他负有保密义务的人员（如职业经理人、技术、采购、销售等涉密重点岗位人员），可与其签订竞业限制协议（见附录 C）。

5.1.1.3 涉密重点岗位员工入职前宜做背景调查，必要时应要求其作出不侵犯他人商业秘密的承诺。

5.1.1.4 在录用潜在竞争性关系企业的员工时，宜采取的措施有：

a) 审核待录用的员工与原单位之间的保密约定、保密义务、保密内容及范围，以防范该员工在本企业内部公开或使用原单位的商业秘密；
b) 提醒待录用的员工不应将原单位的商业秘密带入本企业进行使用或公开，并要求就本项内容签署保证书；
c) 定期对已入职的员工所从事的业务内容进行审核，以排除使用原单位商业秘密；
d) 其他措施。

5.1.2 培训管理

5.1.2.1 商业秘密保护培训宜列入企业年度培训计划，使在职员工对商业秘密可能泄露的异常状态及承担法律后果保持足够警觉。

5.1.2.2 应对新入职涉密岗位的人员进行商业秘密保护培训。

5.1.2.3 可采取发放资料、集中培训、网络培训或相结合的方式开展培训，保存培训记录。

5.1.2.4 签订员工保密合同/协议的人员在培训结束后宜进行考核，保存相关考核材料。

5.1.3 履职管理

5.1.3.1 应督促员工遵守企业商业秘密保护制度，做好本岗位商业秘密保护工作：

a) 涉密信息及载体应及时上报，由保密员归档统一管理；
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。

5.1.3.2 应对员工进行监督，防止在职员工未经商业秘密保护部门审批出现下列行为：

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等。

5.1.4 离职管理

5.1.4.1 涉密岗位员工离职前，企业应主动告知保密义务，以及若违反规定应承担的相应法律责任。告知离职员工不应有以下行为：

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、使用商业秘密等。

5.1.4.2 提醒离职员工主动移交一切涉密载体和物品：

a) 涉密文件资料、数据及其载体、物品；
b) 账号、密码等账户信息；

c） 工作电脑；
d） 门禁卡、钥匙等。

5.1.4.3 宜对其采取适当措施进行脱密，及时回收系统权限，并及时通知与离职员工有关的供应商、客户、合作单位等，做好业务交接。

5.1.4.4 宜开展离职检查，检查内容包括：

a） 检查工作电脑数据是否完整；
b） 检查工作账户：
1） 近期是否有异常操作，如异常查询、下载、拷贝、修改、删除等；
2） 邮箱邮件收发记录。
c） 离职前一定期限内的涉密文档、数据的查阅和使用情况等。

5.1.4.5 宜与离职涉密重点岗位员工签订竞业限制协议等商业秘密保护确认文书，竞业限制协议应根据企业需要进行启动或解除。

5.1.4.6 应及时掌握离职员工在竞业限制期限内的任职去向。

5.2 涉密信息保护

5.2.1 文件资料管理

5.2.1.1 应有密级、保护期限等标识，实行登记管理、归档存放，宜以发文形式公布。

5.2.1.2 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。

5.2.1.3 复制（复印、打印、扫描、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。

5.2.1.4 新闻发布、论文发表、专利申请等信息发布和公开前，由商业秘密保护部门对信息进行审核。

5.2.2 账户、电子信息管理

5.2.2.1 一般要求

5.2.2.1.1 应充分考虑设备、系统的安全性，做好账户、密码的收集、存放和传输的安全工作。

5.2.2.1.2 做好病毒防范和病毒库的升级、查杀病毒等工作。

5.2.2.1.3 定期进行安全检查，发现系统漏洞及时修补。

5.2.2.1.4 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。

5.2.2.2 权限管理

5.2.2.2.1 应对设备、数据库和各类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“最小够用”原则设定权限：

a） 合理分配不同层级账户的功能和审批权限；
b） 合理分配项目中不同账户的功能和使用期限；
c） 合理设定不同账户的访问、操作、查看等权限及其使用期限；
d） 合理设定不同账户的互联网使用权限等。

5.2.2.2.2 权限到期、人员转岗、项目或事项变更时应重新授权。

5.2.2.2.3 人员离职时应回收相应权限。

5.2.2.3 口令管理

5.2.2.3.1 各类设备、数据库和应用系统应设账户和密码，不应使用默认密码或保存密码自动登陆。

5.2.2.3.2 根据企业的业务类型，采取适当的账户、密码管理方式，如：

a) 限制使用简单密码；
b) 必要时不定期更改密码；
c) 输错密码一定次数锁定账户。

5.2.2.3.3 宜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。

5.2.2.4 电子信息保护

5.2.2.4.1 涉密数据应存储于企业授权的存储设备和应用系统，不应存储于非授权存储设备、网络空间。核心秘密、重要秘密等级的数据应采用加密方式存储。

5.2.2.4.2 指定专人进行解密操作，员工按照权限使用加密数据。

5.2.2.4.3 员工需要超出权限查阅或使用加密数据的，应履行审批手续。在查阅或使用完成后，应予以删除，不应非工作需要而擅自使用。

5.2.2.4.4 宜在各类场景进行保密义务提醒，如：

a) 在账户登陆提示、账户登陆后的主界面设置保密义务提醒；
b) 在涉密电子文档首页、页眉、页脚、页面水印等设置保密义务提醒；
c) 在涉密音视频开头提示保密义务。

5.2.2.4.5 定期对涉密数据进行备份并妥善保存。

5.2.2.5 电子信息流转

5.2.2.5.1 收发涉密数据应使用唯一出入口，对涉密数据流入流出进行审批。

5.2.2.5.2 内部局域网应与互联网隔离，涉密数据网络传递应通过内部局域网或加密互联网通道完成。

5.2.2.5.3 通过邮件发送涉密数据时，应加密和签名，可限定文档打开次数、打开时限和编辑权限等。

5.2.2.5.4 对外发送涉密数据应经过审批，并采取加密措施，数据发送与密钥发送不宜采用同一通道。

5.2.2.5.5 应与客户、合作单位等涉密数据接收单位或个人签订保密协议。

5.2.2.5.6 应对涉密数据拷贝采取限制措施，经审核批准后方可拷贝，妥善保存拷贝记录。

5.2.3 其他涉密载体、涉密物品管理

5.2.3.1 涉密信息存放的硬盘、光盘、磁性介质、U 盘等各类存储设备，应妥善保存、归档登记。

5.2.3.2 涉密载体、物品的存放地点宜设为涉密重点区域，宜采取物理隔离的方式进行保护。

5.2.3.3 宜对重要原料和部件实行编号替代、分部门管理等管理方式。

5.2.3.4 未经商业秘密保护部门审批，不准许拍摄、测绘或仿造。

5.2.3.5 由部门保密员登记造册，按权限使用，领用应履行登记手续。

5.2.3.6 跨区域转移应履行审批手续，必要时采取防护措施。

5.2.3.7 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。

5.3 涉密区域管理

5.3.1 应识别涉密区域，区域入口处张贴涉密区域标志和警示语。宜将下列部门或地点列为涉密重点区域：

a) 研发设计、信息管理、财务、人力资源等部门；
b) 实验室、重要生产工作场所；
c) 控制中心、服务器机房等；
d) 涉密档案、涉密载体存放地点；
e) 未公开的样品存放地点；
f) 模具、专用夹具、重要零部件等的存放区；

g） 重要原材料、重要半成品等涉密物资存放区等。

5.3.2 涉密区域宜采取物理隔离保护措施。

5.3.3 涉密重点区域实行进出登记和保密告知，应采取以下保护措施：

a） 划定相对独立的空间，进出口有涉密区域标识；

b） 涉密区域进入需经过授权，设有门禁隔离设施，宜采用指纹、脸部、瞳孔等技术手段验证身份；

c） 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） 限制使用具有录音、摄像、拍照、信息存储等功能的设备；

e） 必要时采取网络隔离阻断等。

5.3.4 涉密区域应限制非相关人员进入，确因工作需要进入的应履行审批手续并全程监督。

5.4 商务活动管理

5.4.1 来访人员访问涉密区域应经审批，履行进出登记，佩戴临时证件。来访人员进入涉密区域，受访部门可设定参观路线，安排人员陪同，限制来访人员使用具有录音、摄像、拍照、信息存储等功能的设备。

5.4.2 在商务合作、共同研究及涉及商业秘密的交易、公证、保险等活动时，应签订保密合同/协议，或在合同/协议条款中规定保密要求，约定保密内容和范围、保密责任和义务及违约责任。

5.4.3 涉及商业秘密的委托加工，应与加工方签订保密合同/协议（见附录 D）或保密条款。

5.4.4 聘任或委托外聘专家、顾问、翻译、律师等可能接触涉密信息的外部人员，宜做背景调查，并签订保密合同、保密条款或保密承诺书。

5.4.5 接受外部单位开展的检查、审计等活动前，应与其签订保密合同或保密条款。

5.4.6 涉及商业秘密的会议或其他活动，应采取下列保密措施：

a） 选择具有保密条件的场所；

b） 根据工作需要，限定参加人员的范围，指定参与涉密事项的人员；

c） 告知参加人员保密要求，必要时签订保密承诺书；

d） 对涉密文件、资料进行控制：

1） 确定文件发放范围，做好发放登记；

2） 重要涉密文件资料应有明显保密和会后回收标识；

3） 休会或会议结束时，及时收回清点、登记。

e） 通过拍照、摄像、签名等方式，做好记录等。

5.4.7 在共同或委托开发的项目合作中应采取措施防止侵犯他人商业秘密，签订保密合同/协议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。

5.5 检查和改进

5.5.1 开展商业秘密保护情况检查，检查内容应包括：

a） 商业秘密保护制度建立情况；

b） 涉密人员管理情况；

c） 涉密区域管理情况；

d） 商业秘密事项的定密、隐密、解密、销毁情况；

e） 涉密文件资料的管理情况；

f） 涉密账户、电子信息的管理情况；

g） 电子邮箱、聊天工具、设计软件、存储软件等工具软件使用商业秘密的情况；

h） 涉密载体、物品的管理情况等。

5.5.2 发现有泄密情况及隐患的，应及时采取纠正/预防措施。

6 商业秘密维权

6.1 应急处置

6.1.1 应制定商业秘密泄密紧急处理预案，建立泄密事件紧急应对流程。

6.1.2 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上级。

6.1.3 出现商业秘密泄露的征兆或者迹象时，企业应：

a) 迅速进行处置，防止信息扩散；
b) 启动对商业秘密泄露的核查、确认和评估，查明原因、责任人；
c) 采取措施，将危害和损失控制在最小限度内等。

6.2 证据搜集

6.2.1 发现商业秘密涉嫌被侵权时，应搜集并整理下列证据性材料：

a) 企业是该商业秘密的权利人的证据：
   1) 泄密信息的具体内容、载体；
   2) 泄密信息为一般公众不知悉或者无法轻易获得的证明；
   3) 已采取的保密措施。
b) 合理表明该商业秘密被侵犯的初步证据：
   1) 泄密人员能够接触秘密信息且被侵权信息与该秘密信息实质相似的初步证据；
   2) 泄密人员相关信息：包括签订劳动合同/保密协议、参与的保密培训、具体工作职责等信息；
   3) 可能的泄密途径。
c) 该商业秘密被侵犯的损害事实：
   1) 侵权行为具体表现（如非法获取、非法披露、非法使用等）；
   2) 被侵权所受的损失或侵权行为所获得收益；
   3) 主张法定赔偿的参考因素及其证据。

6.2.2 可向商业秘密保护服务机构寻求帮助。

6.2.3 可向专业机构申请涉密信息的非公知性、同一性和损失数额的鉴定。

6.3 维权途径

6.3.1 根据证据收集情况，企业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投诉；
b) 向公安机关控告；
c) 申请劳动仲裁或商事仲裁；
d) 向人民法院提起民事诉讼；
e) 向人民检察院提起商业秘密诉讼活动法律监督等。

6.3.2 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。

7 协同保护

7.1 组织保障

7.1.1 企业集聚的园区、特色小镇的管理机构、行业协会和第三方社会服务机构等，可根据自身力量和企业需求，聚集、整合商业秘密保护的服务资源，提供商业秘密保护宣传、咨询、指导、风险监测、维权等服务，为行政部门、司法部门等开展商业秘密保护服务工作提供协助。

7.1.2 园区、特色小镇的管理机构宜设独立的商业秘密保护服务窗口，也可依托知识产权保护服务窗口提供服务。具备条件的园区、特色小镇的管理机构宜设立商业秘密保护服务平台，配置专（兼）职工作人员，建立工作人员管理制度，明确工作职责，保障服务平台正常运营。

7.1.3 园区、特色小镇的管理机构宜积极协调职能部门或社会组织在园区、特色小镇设立商业秘密保护服务指导站。

7.2 服务内容

7.2.1 宣传培训

7.2.1.1 开展商业秘密保护宣传，可采取的方式为：

a) 举办商业秘密保护培训班、讲座；
b) 编制、印发商业秘密保护宣传资料；
c) 利用媒体平台宣传等。

7.2.1.2 提供适合企业不同层次人员的商业秘密保护专题培训：

a) 对企业股东、高级管理人员开展商业秘密保护重要性、必要性和战略性的培训；
b) 对企业从事商业秘密保护工作的专（兼）职人员、重点岗位人员开展商业秘密保护实务及案例培训；
c) 对企业员工开展商业秘密保护知识培训和警示教育；
d) 利用行业协会、学会、商会等渠道将维权成功的案例向企业广泛宣传等。

7.2.2 指导服务

7.2.2.1 通过走访调研，了解企业商业秘密保护需求，有针对性地开展商业秘密保护指导工作。

7.2.2.2 接待和解答企业商业秘密保护咨询，提供商业秘密保护相关资料查询服务。

7.2.2.3 对企业商业秘密保护工作进行风险评估，发现商业秘密保护工作的漏洞。

7.2.2.4 引导企业建立和完善商业秘密保护工作体系，包括：

a) 界定商业秘密保护范围；
b) 建立和完善商业秘密保密制度；
c) 建立和完善商业秘密分级分类管理制度；
d) 建立和完善商业秘密使用管理制度；
e) 建立和完善商业秘密保护的应急反应机制等。

7.2.2.5 第三方服务机构可依相应服务资质提供下列专业服务：

a) 开发、部署和维护涉密文件、数据的信息管理系统；
b) 提供技术信息的非公知性、同一性和损失数额的鉴定评估；
c) 提供科技查新委托服务；
d) 协助被侵权企业搜集证据和维权；
e) 其他专业服务。

7.2.3 风险监测

7.2.3.1 对辖区/行业内商业秘密侵权突发事件、隐患、可能出现的紧急情况开展风险监测。

7.2.3.2　根据发生的商业秘密侵权案例、服务过程中发现的商业秘密泄露隐患，向企业发布商业秘密风险警示。

7.2.4　协助维权

7.2.4.1　当企业反映商业秘密被侵犯并寻求帮助时，提供协助搜集、整理维权材料等服务。

7.2.4.2　根据被侵权企业意愿，协助执法部门开展泄密核查、现场检查等行动，并配合做好调解服务。帮助企业制定维权方案，联系和协调有关部门。

附 录 A
（资料性附录）
商业秘密保密范围

A.1 技术信息

商业秘密的技术信息保护范围的参考内容见表A.1。

表A.1 涉密技术信息

项 目	表现形式
设计信息	设计图及其草案、模型、样板、设计方案、测试记录及数据等。
采购技术信息	型号、牌号、定制品技术参数及价格、特别要求等。
生产信息	产品的配方、工艺流程、技术参数、电子数据、作业指导书等。
设备设施信息	涉密生产设备、仪器、夹具、模具等中的技术信息。
软件程序	设计计划、设计方案、源代码、应用程序、电子数据等。
其他	企业认为有必要采取保密措施的其他技术信息，如未公开的专利申报信息等。

A.2 经营信息

商业秘密的经营信息保护范围的参考内容见表A.2。

表A.2 涉密经营信息

项 目	表现形式
管理文件	文件、规章制度等。
决策信息	战略决策、管理方法等。
研发信息	研发策略、研发经费预算等。
采购经营信息	采购渠道、采购价格、采购计划、采购记录等。
营销信息	营销策划、营销方案、营销政策、营销手册、物流信息、快递信息等。
招投标信息	标书、标底等。
财务信息	财务报表、财务分析、统计报表、预决算报告、各类帐册、工资信息等。
供应商和客户信息	名称、联系人、联系方式、交易习惯、合同内容、交提货方式、款项结算等。
销售信息	销售记录、销售协议等。
人力资源信息	员工名册、职位、联系方式等。
其他	企业认为有必要采取保密措施的其他经营信息。

附 录 B
（资料性附录）
员工保密合同（参考文本）

合同编号：

XXXX保密合同[ ] 号

商业秘密权利人（用人单位）： （下称甲方）

统一社会信用代码：

劳动者或聘用人员： 性别： 年龄： 岁 （下称乙方）

身份证号： 手机：

岗 位： 职务：

家庭住址：

现在住所：

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。

一、入职告知：

1．乙方在进入甲方工作单位之前，对曾经工作过的任何单位或合作单位，均未承担任何保密义务，诸如不泄露、不使用前单位（指与乙方签订有保密协议、竞业限制协议的甲方之前的单位）商业秘密等义务，也未承担任何竞业限制义务。

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，乙方则应保证：

(1)严守对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和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，不从事与其前工作单位具有竞争性质的业务工作。

二、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。

甲方的商业秘密包括且不限于《商业秘密保护范围》（甲方发文公布实施）列出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。

三、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，因此，乙方应严守甲方的商业秘密，并自愿承担保密义务，除因工作需要而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外：

1、严格遵守甲方制定的涉及商业秘密保护的制度（参见合同附件）；

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、不得向第三人提供涉及甲方商业秘密的资料、信息；

9、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；

10、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；

11、其它应当承担的保密义务。

四、成果归属和报告义务：

1、乙方因工作、职务而创造和构思的有关技术和经营的商业秘密或信息归甲方所有；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、乙方在甲方任职期间，完全利用非工作时间，又未使用甲方的资金、技术、商业秘密及工作时间等资源条件，所得的非职务开发结果的知识产权归乙方所有。但以下情况除外：

⑴该研究、开发结果、产品、作品同甲方业务具有竞争性；

⑵实际上或可以论证，该研究、开发结果、产品、作品系抢先占用了甲方的研究、开发结果、产品、作品；

⑶该研究、开发结果、产品、作品系在乙方的职务开发结果的基础上形成的。

3、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。

五、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。

六、乙方承诺：

乙方承诺在甲方工作期间，不得采取下列方式之一披露、擅自使用、或许可第三人使用甲方的商业秘密：

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甲方掌握商业秘密的人员或职员离开甲方；

5、直接、间接、试图影响或者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。

七、保密材料的交还：

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《商业秘密保护范围规定》所列之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。

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。

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。

若乙方擅自带走或不予交还的，视为盗窃商业秘密的行为。

八、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、如果甲方商业秘密进入公知领域，是因乙方的过错，除追究法律责任外，乙方或知悉方仍无权使用该商业秘密。

九、法律责任：

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，为了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，乙方应当向甲方支付违约金为_____万元。甲方遭受到的损失难以计算时，赔偿额为乙方侵权行为所获取的所有经济利益，包括但不限于乙方的工资收入、分红收入或其他一切现实经济收入或可得收入，还包括甲方为获取本合同项下且为乙方违约泄露、使用的商业秘密而付出的开发成本等实际费用。

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，以及因乙方违约给甲方造成的全部直接或间接损失，由乙方承担。

十、争议的解决办法

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，任何一方都有提起诉讼的权利。

十一、本《员工保密合同》(即《保密协议》)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。

十二、本合同一式二份，甲、乙双方各执一份，自签订之日起具有法律效力。

甲方(公章)：　　乙方（签字指印）：

签订地点：

签订日期：　　年　　月　　日

附 录 C
（资料性附录）
竞业限制协议（参考文本）

甲方：

统一社会信用代码：

地址：

乙方： 性别： 年龄：

身份证号： 手机号码：

身份证地址：

现居住地址：

根据《中华人民共和国劳动法》、《中华人民共和国公司法》及有关法律法规，甲、乙双方在平等自愿的基础上，经充分友好协商，就员工竞业禁止等有关事宜，达成如下协议：

1. 乙方承诺，其在任职期间及离职后二年内，不得受聘于任何与甲方业务相同或相似、且有竞争关系的组织，以及从事与甲方业务相同或相似的业务，无论在该组织中任何职，无论全职或兼职；

2. 乙方承诺，其在任职期间及离职后二年内，不得自己经营或与他人共同经营与甲方有直接或间接竞争关系的业务，或在任何直接或间接与甲方竞争的业务中享有任何财务或其他形式的权益。不为与甲方有竞争关系的第三人提供咨询、建议等服务；

3. 乙方承诺，其在任职期间及离职后二年内，不得将自己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自己以前的客户；

4. 乙方承诺，其在任职期间及离职后二年内，不得劝诱甲方员工离职，介绍给与甲方有竞争关系的第三人。

5. 甲、乙双方确认本协议所确定的竞业限制期为乙方在甲方的任期内及离职后二年内。无论乙方因何种原因辞职，本协议之效力均不受影响。

6. 双方确认，竞业限制的范围为 ，地域为 。为补偿乙方离职后二年内的竞业限制义务，甲方支付乙方一定的竞业限制补偿金，在竞业限制期间甲方给予乙方不低于

任职期间月均工资30%的经济补偿，具体标准为　　元/月，在乙方离职后按月打入乙方账户，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。乙方在甲方任职期间甲方不承担任何补偿费用。

7. 乙方如违反本合同任一条款，给甲方造成损失的，乙方应当支付甲方违约金　　元，并承担甲方由此引起的一切损失。损失无法计算时，最低按赔偿甲方人民币　　元计算，甲方因调查乙方的违约行为而支付的合理费用，应当包含在损失赔偿额之内。如乙方的违法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。

8. 因本协议履行过程中发生的纠纷，双方协商解决，协商不成，交由甲方所在地人民法院管辖。

9. 本协议自双方签字或盖章之日起生效。

10. 本协议一式两份，双方各执一份，效力相同。

甲方：　　乙方：

_____年___月___日　　_____年___月___日

签订地点：

附 录 D
（资料性附录）
委托加工保密合同（参考文本）

甲方（委托方）：

住址： 法定代表人：

乙方（加工方）：

住址： 法定代表人：

甲乙双方因委托加工合作涉及甲方商业秘密，为保证甲方商业秘密不受侵犯，经协商一致同意签订本合同，共同信守以下条款做好保密工作。

第一条 委托加工涉及甲方的商业秘密包括：

1、产品（含不合格产品）、样品、包装；

2、工艺资料、图纸、色版/样、原材料配方；

3、委托加工过程中知悉的甲方产品和工艺创造技术、产品价格、供货商、客户等相关信息；

4、委托加工过程中根据甲方产品和工艺创造的新的技术信息、技术资料、知识产权等智力成果；

5、经甲乙双方在委托加工过程中确认的需要保密的其他信息。

第二条 甲方对委托乙方加工所交付的所有标的物享用所有权。

第三条 甲方责任：

1、甲方提供乙方加工需要的技术图纸和加工要求；

2、甲方在以书面、电子(包括：邮件、传真、U 盘等)或其他形式向乙方提供图纸时，需进行登记或备案；

3、甲方对乙方提供的注明保密的技术负有保密责任，未经乙方同意不得提供给任何第三方；

4、甲方在乙方返还属于甲方的标的物时，确认数量并登记或备案。

第四条 乙方责任：

1、乙方应将甲方提供的资料信息仅用于甲方的产品；

2、乙方不论委托加工工作完成与否，都应对本合同中甲方提供的所有标的物严格保密，未经甲方书面同意，乙方不得故意或疏忽以泄露、告知、公布、发布、出版、传授、转让等任何方式将甲方商业

秘密透露给第三方知悉，或自行使用；

3、乙方为承担本合同约定的保密责任，应妥善保管有关的文件和资料，未经甲方事先的书面许可，不得对其复制、仿造等；在委托加工合同到期后，亦不得复制、仿造甲方产品；

4、乙方应当建立商业秘密保护制度，与涉密人员签订保密协议，进行有效管理。建立甲方商业秘密使用台账，确认经手人员、使用时间、产品制作（销毁）数据等情况；

5、乙方应当建立甲方产品废弃物销毁登记制度。乙方销毁甲方的报废品、不合格产品等物品时，需甲方的工作人员或委托人员在场确认；

6、乙方应当于委托加工合同结束时，或者于甲方提出要求后，返还属于甲方的财物标的物。甲方的标的物包括相关图纸资料、加工的报废品、样品、半成品、成品等资料和产品以及记载着甲方秘密信息的一切载体；

7、在本合同约定的保密期限内，乙方如发现甲方商业秘密信息被泄露，应及时通知甲方，并采取积极的措施避免损失的扩大。若商业秘密泄露由乙方造成损失，甲方有权追究乙方法律责任。

第五条　乙方不得利用甲方、甲方产品及提供的资料做宣传。

第六条　乙方在委托加工合同结束后承担保密义务的期限为无限期保密，直至甲方的商业秘密已完全公开公知之日止。

第七条　甲方有权利随时了解乙方对其商业秘密的管理和使用情况。若乙方违反上述条款，乙方将一次性赔偿甲方惩罚性违约金_____元，并赔偿甲方全部经济损失。同时甲方有权单方终止合作关系，并依法追究乙方相关法律责任。

第八条　若因乙方故意或重大过失导致本协议第一条所约定的保密内容对外泄露导致甲方损失的，甲方为维权所支付的合理费用，包括但不限于调查费、差旅费、律师费、诉讼费用等，由乙方承担。

第九条　甲乙双方在委托加工过程中发生纠纷，由双方协商解决或者共同委托双方信任的第三方调解。

若协商、调解未成，双方都有提起诉讼的权利，提起诉讼的法院为甲方企业所在地的各级人民法院，对此条款甲方已特别提醒乙方尽到注意义务。

第十条　本合同的任何修改必须经过双方的书面同意，合同的部分修改或部分无效并不影响其他部分的效力。

第十一条　双方确认，在签署本合同前已仔细审阅过合同的内容，并完全了解合同各条款的法律含义。

第十二条　本合同共一式两份，甲乙双方各执一份。本合同以双方签字或盖章之日起生效。

第十三条　其它未尽事宜，由双方友好协商解决。

甲方（盖章）：　　乙方（盖章）：

法定代表人或委托代理人：　　法定代表人或委托代理人：

签订日期：　　年　　月　　日　　签订日期：　　年　　月　　日

签订地点：