ICS 03.100.01
CCS A 01

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—2022

商业秘密保护管理规范

Management specifications for protection of trade secrets

（征求意见稿）

（本草案完成时间：2022.05.23）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2022－XX－XX 发布　　2022－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

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。

本文件由辽宁省市场监督管理局提出并归口。

本文件起草单位：辽宁省标准化研究院、沈阳鼓风机集团股份有限公司、沈阳新松机器人自动化股份有限公司……。

本文件主要起草人：吕锡源、李洪江……。

归口管理部门：辽宁省市场监督管理局（沈阳市皇姑区崇山中路55号，024-96315-1-2017）

标准起草单位：辽宁省标准化研究院（沈阳市和平区永安北路8号，024-23881581）

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、机构与职责、管理与保护、监督与检查、评价与改进和维权与救济。

本文件主要适用于企业商业秘密的自主管理，科研院所、行业协会等社会组织的商业秘密保护工作参照执行。

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 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。

[来源：中华人民共和国反不正当竞争法，第九条]

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《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释（2020年修正）》。

3.2

涉密资料 secret data

含有商业秘密的纸质文件、电子信息及其载体（电脑、手机、硬盘、光盘、磁性介质、U盘、服务器等）。

3.3

涉密物品 secret items

通过观察或测试、分析手段能够获得商业秘密的生产设备或产品、原材料、半成品和样品等。

4 机构与职责

4.1 企业商业秘密保护管理坚持依法规范、自主负责、预防为主、突出重点、便利工作、合理适当的工作方针。

4.2 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。

4.3 企业的商业秘密保护部门和保密员应履行以下职责：

a) 贯彻落实国家有关商业秘密保护的法律、法规和规章；

b) 执行企业商业秘密保护管理领导机构的决策决议；

c) 确立企业商业秘密保护管理目标；

d) 研究制定企业商业秘密保护管理制度，制度要素见附录A；

e) 组织对企业员工进行商业秘密保护教育培训；

f） 监督检查业务部门落实商业秘密保护管理制度情况；
g） 组织企业内部商业秘密风险隐患排查及应急处理；
h） 开展维权与救济，协助有关部门做好商业秘密侵权事件的调查举证；
i） 做好企业商业秘密保护管理制度体系的评价与改进。

5 管理与保护

5.1 基本流程

5.1.1 定密

5.1.1.1 企业依法确定本企业商业秘密的保护范围，主要包括：
a） 涉密技术信息；
1） 研发信息：与科学技术有关的设计程序、图纸、模型、样板、测试记录、关键信息资源储备、数据等；
2） 生产信息：原料、配方、工艺、流程、样式、技术参数、电子数据、制作方法、技术诀窍等；
3） 配置信息：设备仪器的型号、配置参数、特别要求等；
4） 软件信息：源代码、应用程序、数据算法等；
5） 其他信息。
b） 涉密经营信息；
1） 公司基础信息：公司组织架构、决议文件、内部通知、规章制度、会议纪要等；
2） 决策信息：与经营活动有关的战略规划（计划）、投融资决策、研发策略、商业模式、管理方法、产权交易、股权激励方案、专利规划布局等；
3） 经营信息：产购销计划（方案）、产购销协议、招（投）标标书、产购销记录（订单）、运营成本、内部定价文件、产品合格率、库存量、创意管理等；
4） 客户信息：客户名单、供应商名单、以及对特定客户的网络电子信息、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等；
5） 财务信息：财务账簿、财务报表、融资报表、预决算报告、审计报告、股权分配资料等；
6） 人力资源信息：员工名册、通讯录、工资表、社保公积金清单等；
7） 信息技术信息：应用系统、网络拓扑图、信息安全风险报告、运维日志等；
8） 其他信息。
c） 企业认为应当保护的其他具有价值的商业信息。

5.1.1.2 在生产和经营中，某一信息泄露后会造成下列后果之一的，应列为商业秘密范围：
a） 影响企业生产和发展的事项；
b） 影响企业营销活动的事项；
c） 影响企业技术开发的事项；
d） 使企业在商业竞争中处于被动或不利地位的事项；
e） 使企业经济利益受到损害的事项；
f） 影响企业对外交流和商业谈判顺利进行的事项；
g） 影响企业的稳定和安全的事项；
h） 影响企业对外承担保密义务的事项。

5.1.1.3 下列信息不应作为企业的商业秘密：
a） 公众所知悉的信息；

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。

5.1.2 分级

5.1.2.1 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。
5.1.2.2 企业应建立商业秘密事项目录清单，列明商业秘密的密级、接触人员范围、存放地点、保存方式、保护措施、保密期限、价值估算、泄露损失等内容。
5.1.2.3 对企业商业秘密进行分级、核查和评估时应考虑以下因素：
a） 涉密信息的经济价值；
b） 企业产生涉密信息投入的成本；
c） 涉密信息对企业的重要程度；
d） 竞争对手获取涉密信息后产生的价值；
e） 涉密信息泄漏后造成的经济损失；
f） 涉密信息泄漏后可能承担的法律责任；
g） 涉密信息在企业内部可查阅的范围；
h） 法律、法规、规章及相关司法解释等规定的其他情形。
5.1.2.4 根据 5.1.2.3 规定的因素，企业商业秘密的密级可确定为核心商业秘密、重要商业秘密和普通商业秘密三个保护等级，密级标注统一为“核心商密”“重要商密”“普通商密”。实行定期复评、动态调整。
5.1.2.5 企业的商业秘密保护工作应实行分级管理措施：
a） 对涉密资料、涉密物品实行分级管理，按层级经商业秘密保护部门审批；
b） 对涉密场所实行区域分级管理；
c） 对涉密岗位、涉密人员、涉密活动实行分级管理。
5.1.2.6 企业自行设定商业秘密的保密期限。可以预见时限的以年、月、日计，不可以预见时限的应当定为“长期”或者“公布前”。
5.1.2.7 企业商业秘密的密级和保密期限一经确定，应当在秘密载体上作出明显标志。标志由权属（单位规范简称或者标识等）、密级、保密期限三部分组成。

5.1.3 解密

5.1.3.1 企业的商业秘密出现下列情形时，可予解密：
a） 企业认为商业秘密已不再具有保护价值的；
b） 保密期限届满的；
c） 特定因素导致商业秘密被公开的。
5.1.3.2 解密方式可包括：
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。
5.1.3.3 保密期限内解密的，应当以能够明显识别的方式标明“解密”的字样。

5.1.4 变更

企业可根据经营活动实际，自行确定涉密信息的密级、保密期限、知悉范围等变更事项。涉密信息有关事项如需变更的，应经商业秘密保护部门审批后实施，进行登记备案。

5.1.5 销毁

5.1.5.1 销毁涉密资料和涉密物品，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。

5.1.5.2 销毁过程宜采取下列方式进行监督管理：

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、记录等。

5.1.5.3 企业应采取合适的方式妥善销毁涉密资料和涉密物品，包括：

a) 纸质类资料作粉碎性处理；
b) 电子信息类的存储硬盘、光盘、磁性介质、U 盘等介质与信息系统内的记录一并永久删除；
c) 其他合适的方式。

5.2 涉密资料

5.2.1 纸质文件

5.2.1.1 涉密文件资料存放地点和具体管理方式，由企业根据经营活动实际及涉密信息的密级、性质等自行确定。

5.2.1.2 商业秘密保护部门与涉密信息权属部门，应分别建立涉密信息档案，两部门涉密档案应相互对应，内容详实完整。

5.2.1.3 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。

5.2.1.4 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经商业秘密保护部门审批，复制件与原件的密级、保密期限相同。

5.2.2 电子信息

5.2.2.1 存储

5.2.2.1.1 一般要求

涉密信息存储应满足以下要求 ：

a) 存储于企业授权的存储设备、信息系统或云存储平台；
b) 核心秘密、重要秘密等级的数据采用加密方式存储；
c) 定期对涉密数据进行备份并妥善保存。

5.2.2.1.2 物理载体存储

涉密电子信息的物理载体应满足以下要求：

a) 对涉密电子信息物理载体的采购、维护进行归档登记；
b) 选用安全稳定、运转正常的电脑、手机、硬盘、光盘、磁性介质、U 盘等存储介质；
c) 存储介质送外维修前经商业秘密保护部门审批，并使用专业工具擦除介质中的数据。

5.2.2.1.3 信息系统存储

涉密电子信息的存储系统应满足以下要求：

a) 安装防恶意代码软件，及时更新软件版本和恶意代码库；

b） 定期进行安全检查，发现系统漏洞及时修补；
c） 在系统账户登陆提示及账户登陆后的主界面设置保密义务提醒；
d） 对系统中的涉密音视频、涉密电子文档设置保密义务提醒；
e） 用户的操作行为建立日志记录，实时报告登陆、获取信息和异常入侵等行为。

5.2.2.1.4 云存储空间

企业应严格考察云存储平台的保密性、安全性、稳定性，并对云存储使用权限、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进行明确约定。

5.2.2.2 使用

5.2.2.2.1 企业应对设备、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，并在它们之间形成相互制约的关系。

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经商业秘密保护部门审批后重新授权。

5.2.2.2.3 应对所有涉密账户和密码实行统一登记、备案、发放和变更管理。存储口令的文件应采取商用密码加密措施存储、传播，并保证其安全。

5.2.2.2.4 应定期对用户账号进行清查，及时禁用或删除混用账号、测试账号、临时账号等无关账号，及时清理离职人员账号。

5.2.2.2.5 各类设备、数据库和应用系统应设账号和口令，不应使用默认口令或保存口令自动登陆。

5.2.2.2.6 同一用户登录不同处理商密数据的系统应采用不同口令，确保口令唯一性。

5.2.2.2.7 根据企业的业务类型，采取适当的登录管理方式，如：

a） 口令账号启用严格的口令策略，口令长度至少 8 位以上，采用大小写英文字母、数字及特殊字符的组合；
b） 定期更换口令，更换周期不长于一个月；
c） 输错口令一定次数锁定账号。

5.2.2.3 流转

5.2.2.3.1 企业应对涉密数据拷贝采取限制措施，经审批后方可拷贝，妥善保存拷贝记录。

5.2.2.3.2 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登记。

5.2.2.3.3 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，内部局域网应与互联网隔离。

5.2.2.3.4 对商密数据的发送应采取加密措施，数据发送与密钥发送不宜采用同一通道，并对商密数据知悉范围和权限进行控制，限制阅读人员、阅读次数以及阅读期限。

5.2.2.3.5 与外单位之间的涉密数据流转，应与涉密数据接收单位或个人签订保密协议。

5.3 涉密区域

5.3.1 涉密区域识别

应识别涉密区域，宜将下列部门或地点列为涉密区域：

a） 产品研发设计实验室、重要生产场所、信息数据中心；
b） 涉密档案室，财务、人力资源、销售等部门办公室；

c） 涉密的生产设备、产品、原材料、半成品、样品、载体等存放场所；
d） 企业认为其他应列为涉密区域的场所。

5.3.2 涉密区域保护

5.3.2.1 涉密区域宜采取以下保护措施：
a） 与非涉密区域之间设置物理隔离，可视情况增加网络阻断功能；
b） 出入口设置门禁和涉密区域标识；
c） 出入口处安装视频监控和报警装置；
d） 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；
e） 采用指纹、脸部、瞳孔等技术识别手段验证身份；
f） 出入涉密区域的人员履行权限审批和登记手续；
g） 涉密资料、涉密物品的跨区域转移履行权限审批和登记手续；
h） 限制使用具有录音、摄像、拍照、信息存储等功能的设备。

5.3.2.2 企业应根据业务和保密要求的不同，将内部网络划分为不同的网络区域，涉密网络区域宜采取以下保密措施：
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） 内部网络设备不连接外网；
g） 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；
h） 配备独立的网络基础设施，如服务器、防火墙、专线等。

5.4 涉密人员

5.4.1 入职

5.4.1.1 企业与员工签订的劳动合同中应含有保密条款。

5.4.1.2 企业应根据涉密程度等与核心涉密人员、重要涉密人员签订竞业限制协议（见附录 B），协议中应包含经济补偿条款。

5.4.1.3 应对曾在与本企业具有现实或潜在竞争关系的企业工作员工的身份、背景、专业资格和资质等进行审查，审查要素见附录 C；并在劳动合同中增加不侵犯原单位商业秘密承诺的条款，或签订不侵犯原企业商业秘密的承诺函（见附录 D）。

5.4.2 履职

5.4.2.1 保密教育培训

企业应制定年度员工保密教育培训计划，组织新入职员工、核心涉密人员、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。员工教育培训有关材料应进行登记备案。

5.4.2.2 涉密岗位义务

员工应遵守企业商业秘密保护管理制度，做好本岗位商业秘密保护工作。
a） 超权限接触涉密资料、涉密物品应履行审批和登记手续。
b） 涉密资料、涉密物品的使用、存储、流转按规定要求进行。

5.4.2.3 履职监督检查

企业商业秘密保护部门应会同相关部门，定期对在职员工履职过程中，执行企业商业秘密保护管理制度情况进行监督、检查，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) 进入非授权涉密区域；
b) 登陆未授权账户或系统；
c) 以不当方式获取涉密资料、涉密物品；
d) 超范围、超权限获取使用涉密资料、涉密物品；
e) 拍摄、测绘、仿造涉密物品；
f) 复制、发送涉密电子信息；
g) 将涉密电子信息存于未授权载体或网络空间；
h) 披露企业未公开的信息等。

5.4.3 调岗

5.4.3.1 商业秘密保护部门应与调离涉密岗位的员工进行谈话，告知其应承担的保密义务。

5.4.3.2 商业秘密保护部门应监督调离涉密岗位的员工办理涉密资料和涉密物品的交接手续。

5.4.3.3 涉密员工离岗及交接情况应进行登记备案。

5.4.4 离职

5.4.4.1 涉密岗位员工离职前，企业应与离职员工进行离职谈话，明确商业秘密范围，告知其应承担的保密义务，形成谈话记录并签字确认；并提示离职员工不应有以下行为：

a) 复制、拍摄、篡改、损毁、带离涉密资料、涉密物品；
b) 查阅、拷贝、篡改、发送涉密电子信息；
c) 删除、更改涉密账户；
d) 披露、使用商业秘密等。

5.4.4.2 企业应提醒离职员工主动移交一切涉密资料和物品，包括但不限于：

a) 涉密纸质文件、电子信息及其载体、物品；
b) 涉密工作电脑、手机及涉密信息系统的登陆账户、密码；
c) 涉密区域的门禁卡、钥匙。

5.4.4.3 企业应收回离职员工的各项工作权限，并通知有关的供应商、客户、合作单位等，做好业务对接。

5.4.4.4 企业应对离职员工开展离职前检查，检查内容包括：

a) 离职前一定期限内的涉密资料、物品的查阅和使用情况；
b) 检查工作电脑数据是否完整；
c) 检查工作账户近期是否有异常操作，如异常查询、下载、拷贝、修改、删除等。

5.4.4.5 企业应对离职员工已签订的竞业限制协议进行启动或解除确认。

5.4.4.6 企业应及时掌握离职员工在竞业限制期限内的任职去向。

5.5 商务活动

5.5.1 来访人员访问涉密区域应经审批，履行进出登记手续，佩戴临时证件。

5.5.2 来访人员进入涉密区域后，应由陪同人员按照指定路线进行参观活动，活动过程中不应使用具有录音、摄像、拍照、信息存储等功能的设备。

5.5.3 在开展商务合作、共同研究及涉及商业秘密的交易、公证、保险等活动时，应与相关方签订保

密协议，或在合同中设置保密条款，约定保密内容和范围、保密义务及违约责任。

5.5.4 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。

5.5.5 涉及商业秘密的委托加工，应与加工方签订保密协议，或在合同中设置保密条款。

5.5.6 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，并签订保密协议、保密条款或保密承诺书；可要求其使用企业提供的保密电脑，并对信息采取加密等措施保密。

5.5.7 各级国家机关管理部门人员因监督、检查、取证等工作需要，进入涉密区域、接触涉密资料或涉密物品前，企业应向其明示保密义务。

5.5.8 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) 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) 对涉密资料、物品进行控制：
   1) 确定发放范围，履行发放登记手续；
   2) 涉密资料、物品有明显的“会后回收”标识提醒；
   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。

5.5.9 涉及商业秘密的远程工作，宜采取下列保密措施：

a) 经过商业秘密保护部门审批；
b) 对远程网络进行安全鉴别；
c) 规定硬件和软件的支持与维护要求；
d) 规定远程工作的环境安全要求；
e) 授权访问人员，设置访问权限；
f) 配备专用的操作和存储设备，防止使用私有设备处理或存储信息；
g) 进行安全监视和过程审核，形成记录；
h) 远程工作终止时，撤销授权和访问权限；
i) 其他保护措施。

6 监督与检查

6.1 商业秘密保护部门应制定监督检查方案，定期或不定期对企业商业秘密保护管理制度落实情况开展监督检查工作，并形成监督检查结论。

6.2 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。

注：监督检查工作的职责、权限、频次和时限由企业根据实际情况自行决定。

6.3 监督检查内容应包括：

a) 商业秘密的定密、分级、解密、变更、销毁情况；
b) 涉密资料、物品的管理情况；
c) 涉密区域管理情况；
d) 涉密人员管理情况；
e) 涉密活动管理情况；

f） 涉密账户、密码的管理情况；
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） 企业认为其他应列为监督检查的内容。

6.4 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和系统使用记录；
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） 调取涉密商务活动记录及附属合同。

7 评价与改进

7.1 评价

7.1.1 企业应根据监督检查结论评价商业秘密保护管理制度的有效性，并形成评价报告。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；

7.1.2 企业可根据自身情况，委托律师事务所、司法鉴定所、认证机构等第三方专业机构对企业商业秘密管理进行评价，企业应保留评价记录。

7.2 改进

针对评价报告发现的管理漏洞制定整改计划、采取有效措施持续改进。

8 救济与维权

8.1 应急管理

企业应制定商业秘密泄露的应急预案，建立泄密事件紧急应对流程，包括：成立应急小组、启动泄密溯源、有效制止扩散等。

8.2 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；
b） 对方当事人的信息；
c） 与本企业商业秘密相同或者实质相同；
d） 对方当事人采取不正当手段的事实。

8.3 维权途径

8.3.1 企业的商业秘密被侵犯，可依法采取下列方式进行维权：

a) 向保密行政管理部门举报投诉；
b) 向人民法院提起民事诉讼；
c) 向仲裁机构申请仲裁；
d) 向公安机关报案或控告；
e) 向人民检察院提起商业秘密诉讼活动法律监督。

8.3.2 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。

附 录 A
（资料性）
商业秘密保护管理制度要素

企业商业秘密保护管理制度要素见表A.1。

表A.1 商业秘密保护管理制度要素

制度	要素
商业秘密管理制度	管理目标、管理方针、领导机构、适用范围、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
涉密物理载体管理制度	保护范围、管理单位、使用人员、使用流程、记录存档等
涉密信息系统管理制度	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，保密培训等
涉密商务活动管理制度	访客审批、涉密告知、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

附 录 B
（资料性）
竞业限制协议（参考文本）

甲　　方（用人单位、披露方）：_____
法定代表人：_____ 统一社会信用代码：_____
电　　话：_____ 传　　真：_____
地　　址：_____

乙　　方（劳动者、接受方）：_____
居民身份证号码：_____
电　　话：_____　　职　　务：_____
住　　址：_____

甲、乙双方根据《中华人民共和国反不正当竞争法》《中华人民共和国公司法》《中华人民共和国劳动合同法》及国家、地方有关规定，双方本着平等自愿、协商一致、诚实守信的原则，就竞业限制事宜，于 _____年___月___日（以下简称“生效日”）在中华人民共和国_____（具体签署地址）签署本协议以共同执行：

第一条　合同目的描述

乙方了解甲方就其产品、研发、制造、营销、管理、客户、计算机（程序）、营运模式等业务及相关技术、服务投入庞大资金及人物力，享有经济效益及商誉；乙方若未履行或违反本协议规定，将对甲方投资、经营、商誉或经济权益产生不利影响，甚至产生直接或间接损害，构成不公平竞争，影响产业公平秩序等，甲方将依据中华人民共和国相关法律、法规等追究其相应法律责任。

第二条　竞业限制义务

乙方承诺在竞业限制期间：

1.未经甲方同意，乙方在甲方任职期间不得自营或者为他人经营与甲方同类的营业。不论因何种原因从甲方离职，乙方在劳动关系解除或终止后____年（不超过二年）内，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、从事同类业务的有竞争关系的其他用人单位，或者自己开业生产或者经营同类产品、从事同类业务。

2.乙方为证明在竞业限制期限内已履行了竞业限制义务，自乙方在劳动关系解除或终止后___月内，应及时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，或者能够证明与新的单位存在劳动关系的其他证据；

（2）新的单位为该乙方缴纳社会保险的证明；

（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）或其它公证机构出具的关于乙方的从业情况的证明。

3.不得利用其甲方股东等身份以任何不正当手段获取利益，不得利用在甲方的地位和职权为自己谋取私利。

4.不得直接或间接拥有、管理、经营、控制，或参与拥有、管理、经营或控制或其他任何形式（包括但不限于在某一实体中持有权益、对其进行投资、拥有其管理责任，或收购其股票或股权，或与该实体订立许可协议或其他合同安排，但通过证券交易所买卖上市公司不超过发行在外的上市公司股票3%

的股票的行为除外)从而在竞争性区域内从事与任何在种类和性质上与甲方经营业务相类似或相竞争的业务。

5.不得在竞争性单位或与甲方有直接经济往来的公司、企业、其他经济组织和社会团体内接受或取得任何职务（包括不限于合伙人、董事、监事、股东、经理、职员、代理人、顾问等），或向该类竞争性单位提供任何咨询服务（无论是否有偿）或其他协助。

6.不得利用股东等身份做出任何不利于甲方的交易或安排；不以任何方式从事可能对甲方经营、发展产生不利影响的业务及活动，包括但不限于：利用现有社会及客户资源阻碍或限制甲方的独立发展；对外散布不利于甲方的消息或信息;利用知悉或获取的甲方信息直接或间接实施或参与任何可能损害甲方权益的行为。

7.不得拉拢、引诱或鼓动甲方的雇员离职，且不得自行或协助包括但不限于在生产、经营或销售等领域与甲方经营业务相同及或相似之经济实体招聘从甲方离职之人员。

8.不得在包括但不限于生产、经营及或销售等领域与甲方之包括但不限于原料供应商、产品销售商等各种业务伙伴进行与甲方存在竞争之活动。

9.不得自行或协助他人使用自己掌握之甲方计划使用、或正在使用之一切公开及或未公开之技术成果、商业秘密，不论其是否获得利益。

第三条　竞业限制补偿

1.在乙方竞业限制期间，即与乙方劳动关系解除或终止后____年内，甲方每月向乙方按其离职前12个月平均工资（包括年终奖等一切劳动报酬）的___%的标准支付津贴作为补偿。

2.支付方式为：补偿费从与乙方劳动关系解除或终止之日开始，按月支付，由甲方于每月的__日通过乙方的银行账户支付。乙方银行账户如下：

开户名称：_____

银行帐号：_____

开 户 行：_____

3.如乙方拒绝领取，甲方可以将补偿费向有关机关提存，由此所发生的费用由乙方承担。

第四条　违约责任

1.甲方无正当理由不履行本协议第三条所列各项义务，拒绝支付乙方的竞业限制补偿费（延迟支付约定的补偿费支付期限一个月以上，即可视为拒绝支付）的，甲方除如数向乙方支付约定的竞业限制补偿费外，还应当向乙方一次性支付竞业限制补偿总额___%的违约金。

2.乙方不履行本协议第二条规定的义务,应当向甲方一次性支付竞业限制补偿总额___%的违约金，同时乙方因违约行为所获得的收益应当甲方所有，甲方有权对乙方给予处分。如违约金不足以补偿甲方损失，甲方还有权向乙方主张由此遭受的经济损失。

3.前项所述损失赔偿按照加下方式计算：

（1）损失赔偿额为甲方因乙方的违约行为所受的实际经济损失，计算方法是：因乙方的违约行为导致甲方的产品销售数量下降，其销售数量减少的总数乘以单位产品的利润所得之积。

（2）如果甲方的损失依照第（1）项所述的计算方法难以计算的，损失赔偿额为乙方及相关第三方因违约行为所获得的全部利润，计算方法是：乙方及相关第三方从与违约行为直接关联的每单位产品获得的利润乘以在市场上销售的总数所得之积；

（3）甲方因调查乙方的违约行为而支付的合理费用，包括但不限于律师费、调查费、评估费等，应当包含在损失赔偿额之内。

4.如乙方不能按二条第2项要求提交约定证明材料，则应该视为乙方未履行竞业限制协议约定的义务，甲方有权按本竞业限制协议参考上述条款追究乙方的违约责任。

第五条　合同的权利义务终止

双方约定，出现下列情况之一的，本协议自行终止：

1.乙方所掌握的甲方重要商业秘密已经公开，而且由于该公开导致乙方对甲方的竞争优势已无重要影响。

2.甲方无正当理由不履行本协议第三条的义务，拒绝向乙方支付竞业限制补偿费的。

3.甲方因破产、解散等事由终止法人主体资格，且没有承受其权利义务的合法主体。本合同权利义务的终止不影响甲乙双方在本合同签订之前或之后签订的商业秘密保密协议的效力。

4.竞业限制期限届满。

第六条　纠纷解决程序与管辖

1.对因本协议或本协议各方的权利和义务而发生的或与之有关的任何事项和争议、诉讼或程序，本协议双方均选择以下第____种方式解决：

（1）向本合同签订地人民法院提请诉讼；

（2）向_____仲裁委员会申请仲裁。

2.若协议履行过程中双方发生诉讼或仲裁，在诉讼或仲裁进行期间，除正在进行诉讼或仲裁的部分或直接和实质性地受到诉讼或仲裁影响的条款外，本协议其余条款应当继续履行。

第七条　其他

1.本协议自甲乙双方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：_____

法定代表人/授权代表：_____

日　　期：_____　　日　　期：_____

附 录 C
（资料性）
入职人员审查要素

C.1 在人员入职过程中，应对入职人员进行审查，审查要素包括但不限于：

a) 履历；
b) 教育背景；
c) 专业资质；
d) 与原单位签订保密条款情况；
e) 与原单位签订竞业限制协议情况；
f) 在原岗位涉及知识产权纠纷情况。

附 录 D
（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。

四、本人不会以任何以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。

五、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

参 考 文 献

[1] 中华人民共和国主席令〔2017〕第77号《中华人民共和国反不正当竞争法》

[2] 最高人民法院〔2020〕第19号《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释（2020年修正）》

[3] 国务院国有资产监督管理委员会〔2010〕第41号《中央企业商业秘密保护暂行规定》