ICS 03.100.01
CCS A01

团　　体　　标　　准

T/WLBY 2—2020

企业商业秘密保护工作规范

Specification for the protection of enterprise trade secrets

2020－11－01 发布　　2020－11－15 实施

温岭市泵业协会　　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。

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。

本文件由温岭市泵业协会提出并归口。

本文件起草单位：温岭市泵业协会、利欧集团浙江泵业有限公司、新界泵业（浙江）有限公司、浙江大元泵业股份有限公司、浙江东音科技有限公司、浙江泰福泵业股份有限公司、浙江威格泵业有限公司、温岭市产品质量检验所、浙江台温律师事务所、杭州华知专利事务所、温岭市铁路新区事业发展中心。

本文件主要起草人：叶巧卫、毛剑云、王琳、黄珊、胡小军、吴刚、张行蓉、鲍李丽、金建军、李正宝、季玲行。

本文件为首次发布。

企业商业秘密保护工作规范

1 范围

本文件规定了企业商业秘密管理规范的术语和定义、基本原则、管理机构和职责、商业秘密事项、保密措施、商业秘密维权。

本文件适用于泵与电机类企业商业秘密保护管理，其它企业可参考执行。

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和经营信息等商业信息。

3.2

秘密级商业秘密 secret trade secrets

一般的商业秘密，泄露会使企业的安全和利益遭受损害。

3.3

机密级商业秘密 confidential trade secrets

较重要的商业秘密，泄露会使企业的安全和利益遭受严重的损害。

3.4

绝密级商业秘密 top-secret trade secrets

最重要的商业秘密，泄露会使企业的安全和根本利益遭受特别严重的损害。

3.5

知悉原则 informed principle

根据管理、科研、业务工作的需要，若不向员工授权掌握某项商业秘密就无法进行生产、工作或者达成某项交易，应使其知悉该内容。

3.6

分割原则 division principle

把完整的事项根据经营、管理不同环节分割成若干部分，每个环节只能知悉本部分商业秘密的内容。

3.7

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。

4 基本原则

4.1 商业秘密管理应遵守国家法律、法规、规章规定。

4.2 商业秘密保护以预防为主，遵循需要知悉原则和分割原则，既要保守商业秘密又要有利于开展各项工作。

4.3 商业秘密管理工作实行统一领导、分级管理、分工负责的领导体制和工作机制。

5 管理机构和职责

5.1 企业保密委员会（保密领导小组）

企业保密委员会负责企业商业秘密事项的归口管理工作，负责落实保密管理和技术防范措施，制定保密制度，确定涉密岗位级别，建立商业秘密保护的责任制，负责审批确定企业文件密级，并形成企业各密级文件清单，保持动态管理，负责检查指导企业商业秘密工作情况，决定重大的商业秘密事项决策等。

5.2 企业商业秘密管理办公室（知识产权管理部门或法务部门）

企业商业秘密管理办公室是企业商业秘密的归口管理部门。其主要职责：

a) 宣传贯彻国家保密法规和企业有关保密制度；
b) 组织制定企业商业秘密保护规章制度；
c) 企业商业秘密的管理；
d) 负责出国携带资料或新闻宣传的保密审查；
e) 检查指导计算机信息网络的安全保密工作；
f) 调查处理企业失、泄、窃密事件。

5.3 领导负责制

企业对商业秘密的保护实行领导负责制。

5.4 分工负责制

5.4.1 企业对商业秘密的保护实行分工负责制，遵循“谁主管，谁负责”和“谁涉密，谁负责”的原则。

5.4.2 企业分管保密工作的领导担负具体组织领导的责任，分管有关方面工作的领导负责分管工作范围内的保密工作。

5.4.3 企业各部门负责各自职责范围内涉密事项的保密管理、监督和检查工作，并针对本部门实际业务工作制定专业性保密管理措施。

5.5 企业各部门和商业秘密管理人员

5.5.1 部门负责人

企业各部门负责人为商业秘密保护的第一责任人，负责确定和修改部门商业秘密的事项和范围，并实施有效的管理。

5.5.2 专（兼）职保密员

部门设立专（兼）职保密员岗位。专（兼）职保密员岗位职责应包括：

a) 落实国家及企业各项保密规定，制定本部门保密事项的保密管理制度；
b) 监督检查本部门保密工作，发现问题及时整改；
c) 负责本部门商业秘密的定密、解密的工作；
d) 协助调查处理本部门失、泄、窃密事件；
e) 宣传商业秘密保护的意义、作用，增强全员的保密意识。

5.5.3 企业人力资源部门

5.5.3.1 企业人力资源部门负责开展新员工入职培训，将商业秘密的管理纳入培训内容，并详细说明部门及岗位的涉密内容、管理制度。

5.5.3.2 开展新员工入职背景调查，对签订同行业《竞业禁止协议》等涉密合同的人员在限定期限届满前，不得招聘。

5.5.3.3 负责员工薪酬保密。

5.5.4 企业信息技术部门

企业信息技术部门负责企业涉密网络、信息系统、计算机和移动存储介质的保密管理工作。

6 商业秘密事项

6.1 商业秘密范围

技术类秘密信息保护范围参见表1，经营类秘密信息保护范围参见表2。

表1 涉密技术信息

类 别	表 现 形 式
设计信息	产品设计方案、外形设计方案、流体分析报告、产品图纸、企业产品技术标准、设计评审资料、鉴定验收资料、技术总结、技术通知、模型、自制样机、试验记录、试验报告等。
工艺信息	工艺流程图、工艺文件、检验指导书、小批试制总结报告等。
其 他	涉密非标关键设备的资料、订制品采购的技术参数及价格、特殊要求等。

表2　涉密经营信息

类别	表现形式
管理文件	企业体系内部审核、管理评审报告；企业内部考核体系方案；档案(纸质和电子版)、规章制度、ERP信息资料、服务器备份数据资料、各部门电子档案、电子邮件等。
决策信息	战略决策、管理方法、项目投资策略及方案等。
研发信息	研发策略、研发经费预算等。
采购信息	主要供应商信息、进价策略、采购渠道、主要原材料指标、采购计划、采购记录等。
销售信息	营销计划、营销方案、营销政策、营销手册、销售协议、销售记录等。
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、银行存款核算、往来核算、成本核算、存货核算、长期投资核算、工资核算、销售核算、所有者权益核算、外部会计报告、内部会计报告、股权调整方案、对外交流和商业谈判摘要等。
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。
人力资源信息	企业人力资源计划、人力资源结构、薪酬方案、员工档案、员工名册、职位、联系方式等。
运营信息	企业改革和发展方案、企业技术合作方案、企业突发事件处置方案、企业涉稳事件处置方案、企业突发和涉稳事件处置资料。
其他	企业认为有必要采取保密措施其他经营信息。

6.2　密级

商业秘密按重要程度由低到高依次划分为秘密级、机密级和绝密级。

6.3　定密

6.3.1　定密评估

定密时应从表3的因素考虑泄密后产生的影响。

表 3 涉密影响

序号	因　素	影　响
1	商业价值	现在的和将来的
2	损失	可能造成的损失程度
3	竞争企业	对竞争企业产生的价值
4	合同或法律法规	违反后的法律责任

6.3.2　商业秘密项目的确定程序

6.3.2.1　商业秘密产生部门拟定保密项目，建议保密期限和知悉范围，本部门保密员审核、本部门主要负责人签批确认后，报至企业商业秘密管理办公室。

6.3.2.2　商业秘密管理办公室牵头相关部门、人员对提出的商业秘密确认申请进行论证，并给出论证结果。

6.3.2.3　商业秘密管理办公室根据评估结果，报送企业保密委员会审批后执行。

6.3.2.4　商业秘密管理办公室根据企业规定对审批后的密级文件确认保密期限、知悉范围等。

6.3.3　商业秘密项目变更

6.3.3.1　密级和保密期限确定后，发现下列情形之一的，应及时变更：

a）　泄漏后对企业利益的损害程度发生明显变化的；

b）　因工作需要，原知悉范围有较大变化的；

c）　事项密级或保密期限已经发生变化。

6.3.3.2　变更的流程如下：

a）　涉及商业秘密的部门提出的商业秘密变更和解除申请；

b）　商业秘密管理办公室组织对商业秘密进行评估；

c）　商业秘密管理办公室根据评估结果，出具商业秘密变更、解除意见；

d）　企业保密委员会对变更和解除进行确认审批；

e）　商业秘密管理办公室根据审批的情况，重新确定商业秘密管理台账的状态；

f）　密级、保密期限变更后，涉及商业秘密部门应及时变更标识。

6.4　隐秘

企业在对外公开发布信息或与供应商、客户、合作方、其他单位沟通时应注意隐秘，可对涉密信息进行模糊化技术处理以便隐藏，或者删除涉密信息。

6.5　解密

当保密期限已满，评估商业秘密事项已不再具有保护价值的，或者因特定因素导致商业秘密被公开的应予解密。解密需要对实物和电子版同时消除或涂改密级标识，并移出涉密区域。

6.6　标识

6.6.1　商业秘密应以 3 号方正黑体字，将确定的密级，标注在文件首页左上角。如：绝密、机密和秘密。

6.6.2　绝密级商业秘密文件，应于首页右上角标注文件份数序号。

6.6.3　涉密载体，应在外包装上标明与内容一致的密级。密级标识与涉密载体不得分离。

6.6.4　摘录、引用秘密信息的，应在派生载体上标识与原件一致的密级。
6.6.5　文件资料汇编中有涉密文件的，除对各独立文件的密级做出标识外，还应按照汇编中的最高密级，在封面做出标识。
6.6.6　各部门对商业秘密标识后，应即行登记建立台帐，由专人管理，按企业档案管理有关规定建立查阅、借阅制度。
6.6.7　在特殊情况下未进行标识的有关资料、文件仍然为商业秘密。

7　保密措施

7.1　保密教育

7.1.1　商业秘密保护教育应列入企业年度培训计划，促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。
7.1.2　企业保密办公室组织对中层领导及各部门保密员开展培训教育，再由各部门进行内部培训，采用这样横向纵向相结合的方法，达到全员保密教育，增强保密意识。
7.1.3　保密教育可以采用多种形式，并对结果进行考核，使全体员工自觉遵守保密基本准则。做到不该说的机密，绝对不说，不该看的机密，绝对不看（含超越自己职责和业务范围的所有文件及言谈）。

7.2　奖惩

7.2.1　对员工依照企业规定,在保守企业秘密方面,能忠于职守,从事保密工作取得显著成效的;发现他人泄密,能立即采取补救措施,避免或减轻损害后果的；对泄密或者非法获取企业秘密的行为及时检举、投诉的，按照有关规定给予奖励。
7.2.2　对员工因不遵守企业规定,造成泄密事件,依照有关法规及企业的奖惩制度，给予纪律处分、解雇，直至追究其法律责任。

7.3　人员管理

7.3.1　招聘管理

7.3.1.1　对涉密重点岗位员工入职前宜做背景调查。
7.3.1.2　不应以取得第三方的商业秘密为目的录用竞争性企业的员工。
7.3.1.3　在录用竞争性企业的员工时，宜审核其与原单位之间的保密内容及期限，提醒不应将原单位的商业秘密带入本企业内部进行使用或公开，并要求签署保证书。

7.3.2　入职管理

7.3.2.1　新入职或转岗到涉密岗位的员工，应与其签订员工保密合同（参见附录A）。
7.3.2.2　高级管理人员、高级技术人员及其他负有保密义务的人员可与其签订竞业限制协议(参见附录B)。
7.3.2.3　应对新入职人员进行培训，可集中面试或网络培训的方式进行，培训结束后宜进行考核，并保存培训和考核记录。

7.3.3　履职管理

7.3.3.1　员工应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）　按企业的授权权限查阅使用涉密信息；

b） 按企业规定对办公电脑设置密码和屏幕保护时间，并定期进行更改；
c） 不该看的秘密不看，不该说的秘密不说；
d） 不登录未授权的的账户和系统；
e） 不进入非授权涉密区域。

7.3.3.2 宜对中高层管理人员和涉密重要岗位员工的下列行为进行限制：
a） 兼职、入股、组建、参与组建或变相投资与所在企业经营相类似的企业；
b） 同与所在企业有交易关系、竞争关系的国内外企业进行涉密交易。

7.3.4 离职管理

7.3.4.1 涉密岗位员工离职时，按企业规定首先进行离职检查，检查工作电脑和工作账户，查看是否近期有异常操作和邮件收发记录、近期涉密文件查阅使用情况等。

7.3.4.2 及时销毁账户，收回一切权限，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。

7.3.4.3 企业保密机构应要求离职员工对其在入职、履职以及离职过程中接触或交接的企业商业秘密载体登记记录，知悉的企业商业秘密内容进行确认，并要求离职员工作出书面保密承诺。

7.3.4.4 宜与涉密重点岗位离职员工启动竞业限制，协商确定竞业限制补偿费和违约金。补偿费宜大于劳动合同解除或者终止前十二个月平均工资的 30%，按月支付；员工违反竞业限制约定的，应当按照约定向企业支付违约金。

7.3.4.5 离职表应设置保密人员签字，经签字后方可办理离职手续。

7.3.4.6 涉密员工无法按照正常程序办理离职手续的，企业保密机构、人力资源部门应当在涉密员工离职后，立即收集整理离职员工在入职、履职以及离职过程中接触或交接的企业商业秘密载体登记记录，知悉的企业商业秘密内容，以及离职员工作出承担保密义务的依据。

7.4 涉密信息保护

7.4.1 涉密信息载体

7.4.1.1 建立健全商业秘密载体（纸质、U 盘、光盘、移动硬盘、特定的样机、磁性介质、邮件、微信、QQ 等社交软件传输的文件）的收发登记、签收、催办、清退、借阅、归档制度，由部门专兼职保密员登记造册，按权限使用、查阅、借阅、续借应履行登记手续。

7.4.1.2 制作商业秘密载体，应当进行定密、标密，建立台账，在发放时应严格按批准的范围执行，并作好发放登记管理；制作过程应进行保密，落实专人负责制作、收转、存档。秘密载体原则上应在本单位制作，委托外单位制作应事前签订保密协议或在合同条款中约定保密事项及违约后应承担的责任，制作过程中形成的校样、印版、底片和废品等，应及时专人监督销毁。

7.4.1.3 收到商业秘密载体，应履行清点、签收等手续，并进行商业秘密汇总台帐登记。

7.4.1.4 不得通过普通传真机、公用电子邮件、手机短信、聊天工作、普通邮政传递商业秘密载体。企业部门之间传递商业秘密载体应使用专业办公软件或专人密封报送。

7.4.1.5 机密级和绝密级文件、资料除知悉范围人员外，企业员工查阅须经商业秘密管理办公室或企业保密委员会批准，但不得借出。

7.4.1.6 严禁复制绝密级商业秘密载体。复制机密级以下商业秘密载体，应由本部门负责人审核，经商业秘密管理办公室批准，复制件视同原件进行登记管理；汇编涉密文件、资料，应经商业秘密产生部门许可，汇编成册的文件、资料，应按其中最高密级和最长保密期限进行密级文件管理。

7.4.1.7　保存商业秘密载体，应当选择特定的保密区域或安全保密的场所、部位、设备。管理人员离职前，应办理移交手续。被撤销、合并的单位，应将秘密载体移交承担原职能的单位或保密部门，并履行登记、签收手续。

7.4.1.8　销毁商业秘密载体，须由商业秘密管理办公室审核，经企业保密委员会批准，履行登记手续后，在保密办指定的场所按规定的方法进行，并在专人监督下销毁。纸质涉密文件必须使用碎纸机，未经切碎的文件严禁作收购处理。

7.4.1.9　部门相关人员在指定时间、指定区域使用本部门的商业秘密，确需借出的应经部门负责人批准，并采取安全措施。在经办涉及机密级、绝密级商业秘密文件时，须分别经商业秘密管理办公室和保密委员会审批；结束后应立即将有关资料交本部门负责人审核，并归入本部门档案管理。保密员做好本部门档案资料的统一登记和管理。

7.4.1.10　因工作需要，由员工个人保管的商业秘密载体，需征得部门负责人同意,保密员做好登记,保管人应严格履行保密职责。企业员工本人工作所持有的各种文件、资料、电脑复印件,应妥善保管,未经批准不能携带外出。

7.4.1.11　企业各类商业秘密载体，除按有关规定上报主管部门、传送应知单位和按合同或协议规定交付有关单位外，任何单位、个人不得以任何形式向外单位或个人提供、传递、复制、摘抄、转让和使用。

7.4.1.12　企业各类商业秘密载体不得随意摆放在公共区域。

7.4.1.13　企业工作人员因公出差，不得携带涉及商业秘密的文件、资料、软盘和其他介质。对确属工作需要携带的，须经本部门负责人同意，商业秘密管理办公室审核。出差期间要增强安全防范意识，妥善保管，回单位后要及时交还。

7.4.1.14　凡商业秘密文件、资料、软盘和其他介质不得携带和邮寄出境。特殊情况下确需携带的，必须履行保密审查手续，属秘密级的企业商业秘密管理办公室审核批准，属机密级、绝密级的由企业保密委员会审核批准。

7.4.1.15　经批准同意携带出境的商业秘密文件、资料，要采取严格的保护措施，妥善保管，防止泄露和丢失，回国后及时交还。

7.4.2　电子信息保护

7.4.2.1　涉及商业秘密的电子信息在制作过程和生成后的保护均通过网络权限的设置进行。

7.4.2.2　涉密数据应存储于企业授权的存储设备和应用系统，机密、绝密数据应采用加密方式存储。

7.4.2.3　定期对涉密数据进行备份并妥善保存。

7.4.2.4　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完成。

7.4.2.5　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，不准许非工作需要而擅自使用。

7.4.2.6　对涉密办公电脑封锁 U 盘接入口，禁止复制流转。

7.4.2.7　涉密信息需要对外流转时，应经过审批，由指定专人进行解密操作方可传输。

7.4.2.8　应与客户、合作单位等涉密数据接收方签订保密协议。

7.4.3　网络

7.4.3.1　一般要求

7.4.3.1.1　做好账户、密码的收集、存放和传输的安全工作。

7.4.3.1.2　做好病毒防范和病毒库的升级、查杀病毒等工作。

7.4.3.1.3　信息化部门做好 24 小时无间断值班，及时处理异常，保障设备、系统的安全，运行平稳。

7.4.3.1.4 总机房做好晨检，检查服务器、核心交换机、防火墙、UPS、空调、报警器等所有机房内设备设施的运行情况及灰尘、温度、湿度等机房环境情况，并填写机房晨检纪录表。若出现异常需及时上报。

7.4.3.1.5 分机房每周检查一次，做好数据备份；每半年对所有设备进行系统的检查。

7.4.3.1.6 用户的操作行为应有日志记录，可实时报告异常入侵、登陆、获取信息的行为。

7.4.3.2 计算机设备及网络权限

7.4.3.2.1 所有员工一律使用企业配置的计算机，严禁携带个人计算机进入办公区域。计算机经信息化部门固定后，严禁私自移动和拆机。因工作原因需携带计算机离开办公区域，必须由部门主管批准，且经信息化部备案。

7.4.3.2.2 对计算机控制 USB 接口，各系统只有分管领导、部门负责人可开通计算机 USB 接口，部门负责人助理或其指定一位可开通，但重点关注，其他人员 USB 接口均为禁用状态，因工作需要确需拷贝资料，需部门负责人审核相应资料文件后由未禁用 USB 人员处拷贝，原则上不允许资料拷贝。

7.4.3.2.3 应对外网、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。

7.4.3.2.4 外网权限，部门负责人经分管领导批准后可按需求开通；项目经理原则上不允许开通， 确有需要经部门负责人批准后可开通工作日上班时间段；其他人员不允许开通外网，如需查询资料可通过有外网同事进行；资料与行政管理员仅开通与工作有关的外网；除上述外的其他辅助性岗位确有外网需要需经部门负责人批准后开通，但该岗位将纳入重点关注对象。

7.4.3.2.5 企业员工均需接入企业局域网工作，不得私自更改 IP 地址。图文档系统、生产 SAP 系统、财务系统等各个分系统局域网以及外网使用的权限均通过流程申请，信息化部门根据审核结果进行指定权限的开通。

7.4.3.2.6 全企业安装计算机监控软件，各分系统领导和部门负责人可监控下级计算机操作过程；所有人员电脑均需安装监控客户端，不得私自卸载。

7.4.3.2.7 研发图文档系统，资料与行政管理员拥有 PDM 软件中管理员级权限；其他人员文档树仅有查看、复制、粘贴权限，结构树按照软件中设定角色权限；所有人员一人一账号，不得使用他人账号，不得将账号借于他人使用。

7.4.3.2.8 权限到期、人员转岗、项目或事项变更时应重新授权。

7.4.3.2.9 人员离职时应回收相应权限。

7.4.3.3 口令管理

7.4.3.3.1 各类数据库和应用系统应设账户和密码。

7.4.3.3.2 密码通常应包含数字和字母且不少于 6 位的中等复杂程度密码，禁止使用默认密码、出生日期或 123456 等简单密码或保存自动置附，并按规定时间间隔进行密码更改。

7.4.3.3.3 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。

7.5 涉密区域

7.5.1 宜将下列部门或地点列为涉密重点区域：

a） 研发设计、财务；

b） 实验室、重要生产场所；
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） 重要样机的存放区。

7.5.2 涉密区域宜有明显标识和警示语，宜采取物理隔离保护措施。

7.5.3 涉密重点区域进出实行门禁管理。

7.5.4 限制使用具有录音、摄像、拍照、信息存储等功能的设备。

7.5.5 必要时采取网络隔离阻断。

7.5.6 涉密区域限制外来人员访问、参观、考察，确因工作需要进入的应履行审批手续并全程监督。

7.5.7 涉密区域宜设置电脑录屏。

7.6 商务活动管理

7.6.1 参观访问，应合理规划线路，尽量避开涉密区域,应由指定人员陪同；如需访问涉密区域，需经过审批，禁止参观人员携带手机、相机、录音笔等有信息存储功能的设备。

7.6.2 涉及商业秘密的会议或其他活动，应采取具有保密条件的场所，参加人员必要时签订保密承诺书，通过拍照、摄像、签名等方式，做好记录。会议重要涉密文件资料应有明显保密和会后回收标识，休会或会议结束时，及时收回清点、登记。

7.6.3 在商务合作、共同研究及涉及商业秘密的交易活动时，应签订保密合同，在合同条款中规定保密内容、范围、责任和义务及违约责任。书面明确利用合作方或己方提供的秘密信息开发所得成果的所有权与使用权，防止本企业自行研究、开发活动中带入合作方秘密信息。

7.6.4 聘任或委托的外聘专家、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，并签订保密合同协议。

7.6.5 在收购技术和客户名单等经营信息时，通过尽职调查、合同条款约束等方式确保出售方对出售标的享有充分有效的处置权。

7.6.6 涉及商业秘密的委托加工，应与加工方签订保密协议（参考附录 C）。

7.7 检查和改进

7.7.1 应进行年度定期检查和不定期抽查，检查内容如下：
a） 商业秘密保护规章制度建立和实施情况；
b） 涉密人员培训、管理等情况；
c） 涉密区域管理情况；
d） 涉密信息传输情况；
e） 涉密文件资料的管理情况；
f） 涉密载体、物品的管理情况；
g） 商业秘密事项的定密、隐秘、解密情况。

7.7.2 发现有泄密情况及隐患的，应及时采取纠正。

8 商业秘密维权

8.1 应急处置

8.1.1 参照附录 D 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。

8.1.2 当发现有泄密迹象时，启动应对流程，防止进一步扩散和损失进一步扩大，将危害控制在最小限度内。

8.2 证据搜集

8.2.1 发现商业秘密涉嫌被侵权时，应搜集并整理以下证据性材料：

a） 侵权主体信息；
b） 侵犯涉密信息的具体行为表现；
c） 侵权后果，即侵权行为导致本企业的损失情况，及可能导致的后果；
d） 可能与泄密信息有关的人员情况（单位、保密合同/协议、工作经历、社会关系）；
e） 泄密信息的具体内容、载体、途径；
f） 企业已采取的保护措施；
g） 泄密信息具有现实或潜在的商业价值；
h） 泄密信息的权属。

8.3 技术支持

8.3.1 可向商业秘密保护服务机构寻求帮助。

8.3.2 可向专业机构申请涉密信息的非公知性、同一性、价值性鉴定。

8.4 维权途径

8.4.1 根据证据收集情况，企业可依法采取下列方式进行维权：

a） 与侵权人协商和解；
b） 请求调解组织调解；
c） 向市场监督管理部门投诉；
d） 涉及劳动关系的可向劳动仲裁机构申请仲裁；
e） 根据仲裁条款或达成的仲裁协议提请仲裁机构仲裁等；
f） 涉嫌犯罪的可向公安机关举报、控告；
g） 向人民法院提起诉讼；
h） 申请人民检察院对商业秘密诉讼活动进行监督等方式进行维权。

附 录 A
（资料性附录）
员工保密合同

甲方：
联系电话：
乙方：
性别：
身份证件号码：
户籍地址：
通讯地址：
联系方式：

甲乙双方就乙方在任职期间及离职以后的保密及竞业限制事宜，达成以下条款，以共同遵守：

第一条 秘密信息

甲乙双方确认：“秘密信息”是指甲方及其关联企业未曾公开的商业秘密、技术信息和财务信息等，包括但不限于设计、程序、制作工艺、制作方法、管理诀窍、产品或服务的销售网络、销售状况、客户名单、市场开发及售后服务情况、产销策略、招投标中的标底及标书内容。

乙方承认在为甲方工作期间可能直接或间接地通过书面、口头、图表、音像资料等获得或通过观察全部或部分设备、产品等获得这些秘密信息。

甲乙双方同意，上述“秘密信息”不包含那些非因乙方过错而进入公众领域的公开信息。

第二条 对秘密信息的保密

乙方承诺，严格保守自己在为甲方工作期间所获得有关甲方及甲方项目的一切秘密信息。

乙方保证除非为了甲方项目的工作需要交流此种秘密信息外，未经甲方事先书面许可，不以任何方式，无论口头、书面，还是磁盘、通信网络等介质向任何其他方，包括个人、企业、商社、其他经济组织等泄露秘密信息。

第三条 禁止非法使用秘密信息

乙方保证除非为了甲方项目的工作需要而使用此种秘密信息履行职务外，未经甲方事先书面许可，不以任何方式自行使用秘密信息，并且不以任何方式许可或协助他人使用秘密信息。

第四条 秘密信息的停止使用

在甲、乙双方劳动关系无论何种原因终止或解除后，乙方应停止使用所有的秘密信息，而且只要此种秘密信息尚未依法进入公众领域，乙方就不得继续使用，也不得向任何个人、企业、商社、其他经济组织等披露此种秘密信息。

在甲、乙双方的劳动关系存续期间及终止或解除后，一旦甲方要求，乙方应随时将从甲方及甲方项目获得的一切资料文件及其复制件归还甲方或进行销毁。

第五条 保密期限

双方同意本协议规定的保密期限为自本协议签署之日起至双方劳动关系终止或解除后年内有效。

在保密期限内，乙方无论因何种原因从甲方或甲方关联企业离职，仍须承担如同任职期间一样的保密义务；乙方认可，甲方及甲方关联企业在支付工资报酬时，已考虑了乙方离职后需要承担的保密义务，故而无需在乙方离职时另外支付保密费。

第六条 违约责任

如果乙方违反本协议的规定，应赔偿甲方全部损失。赔偿范围包括但不限于甲方的名誉损失、直接损失和可得利益的损失，以及调查费用和诉讼费用、律师费用。

乙方违约后还应采取各种合理方法挽回泄密造成的影响，尽可能使秘密信息继续处于保密状态；同时，本协议继续有效。

乙方违反本协议任何条款的行为均视为严重违反劳动纪律和甲方规章制度，无论违约金及损失赔偿金给付与否，甲方均有权不经预告立即解除与甲方的聘用关系。

第七条 协议的生效与效力

1、本协议自甲、乙双方签字之日起生效。

2. 双方就履行中产生的任何争议，应通过友好协商解决，协商不成，任何一方有权向人民法院提起诉讼。

2、本协议一式二份，甲、乙双方各执一份，具有同等法律效力。

甲方（盖章）：　　乙方（签字）：

签订日期：　　年　月　日

附 录 B
（资料性附录）
竞 业 禁 止 协 议 书

甲方（用人单位）：

乙方（劳动者）： 身份证号：

乙方已同甲方签订劳动合同，且为甲方员工，因工作需要，接触到甲方的商业秘密，为保护甲方的商业秘密及其合法权益，确保乙方在职期间和离职后不与甲方竞业，甲、乙双方根据《中华人民共和国劳动合同法》等法律法规，在遵循平等自愿、协商一致、诚实信用的原则下，就乙方对甲方承担的竞业限制义务及甲方因乙方承担竞业限制义务而对乙方的补偿等相关事项达成如下协议：

一、未经甲方同意，乙方在任职期间不得从事以下行为：

1、自己开业生产或经营与甲方生产或经营产品同类的产品；

2、自营与甲方同类的业务；

3、为他人经营与甲方生产或经营的产品同类的产品；

4、为他人经营与甲方同类的业务。

二、乙方离职后的竞业禁止义务

1、不论因何种原因从甲方离职，乙方应立即向甲方移交所有自己掌握的，包含有职务开发中商业秘密的所有文件、记录、信息、资料、器具、数据、笔记、报告、计划、目录、来往信函、说明、图样、蓝图及纲要（包括但不限于上述内容之任何形式之复制品），并办妥有关手续，所有记录均为甲方绝对的财产，乙方将保证有关信息不外泄，不得以任何形式留存甲方有关商业秘密信息，也不能得以任何方式再现、复制或传递给任何人，更不得利用前述信息谋取利益。

2、不论因何种原因从甲方离职，离职后2年内不得参与甲方从事的行业相同或相近的企业，及与甲方有竞争关系的企业内工作。

3、不论因何种原因从甲方离职，离职后2年内不得自办与甲方有竞争关系的企业或者从事与甲方商业秘密有关的产品的生产。

4、在与甲方离职后2年内，不能直接地或间接地通过任何手段为自己、他人或任何实体的利益或与他人或实体联合，以拉拢、引诱、招用或鼓动之手段使甲方其他成员离职或挖走甲方其他成员，不得劝说、诱使、抢夺甲方客户或潜在客户。

5、从乙方离职后开始计算竞业限制期，甲方向乙方支付补偿费。如乙方拒绝领取，甲方可以将补偿费向有关方面提存。

6、竞业禁止期满，甲方即停止补偿费的支付。

7、乙方应于每月20日前告知甲方其现在的住所地址、联系方法及工作情况，甲方可以随时去乙方的住所处核实情况（包括查看乙方的住所地的房屋租赁合同或房产证和向乙方邻居了解乙方的工作情况），乙方应当予以积极配合。

三、违约责任

1、乙方不履行规定义务的，应当承担违约责任，违约金需一次性向甲方支付,违约金额为乙方离开甲方上年度的薪酬总额的3倍。同时，乙方的违约行为给甲方造成损失的，乙方应当赔偿甲方的损失，并且乙方所获得的收益应当全部归还甲方。

2、甲方不履行规定义务的，应当依照法律规定承担违约责任。

四、争议解决

因履行本协议发生的劳动争议，双方应以协商为主，如果无法协商解决，争议一方或双方有权向甲方所在地的劳动争议仲裁委员会申请仲裁。

五、其他

1、本协议提及的技术秘密，包括但不限于：技术方案、工程设计、产品设计、制造方法、产品材料构成、工艺流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、实验数据、试验结果、图纸、样品、样机、模型、模具、操作手册、技术文档、相关的函电等等。

2、本协议提及的商业秘密，包括但不限于：客户名单、行销计划、采购资料、定价政策、 财务资料、进货渠道等等。

3、本协议未尽事宜，或与今后国家有关规定相悖的，按有关规定执行。

4、本协议及甲乙双方所签订的《保密协议》作为劳动合同附件，经甲乙双方签字盖章后，具有同等法律效力。

5、一式两份，甲乙双方各持一份，具有同等法律效力。

甲方：	乙方（员工）（签字）：
地址：	住址：
法定代表人：	职务：
签署人签字：	电话：
电话：	身份证号码：

附 录 C
（资料性附录）
委托加工保密协议

甲方：

乙方：

因乙方现正在为甲方提供服务和履行职务，已经（或将要）知悉甲方的商业秘密。为了明确乙方的保密义务，有效保护甲方的商业秘密，防止该商业秘密被公开披露或以任何形式泄露，甲、乙双方本着平等、自愿、公平和诚实信用的原则签订本保密协议。

第一条 秘密信息

1、本协议所称秘密信息包括：技术信息、专有技术、经营信息和甲方企业中列为绝密、机级的各项文件。乙方对此商业秘密承担保密义务。

本协议之签订可认为甲方已对企业的商业秘密采取了合理的保密措施。

2、技术信息指甲方拥有或获得的有关生产和产品销售的计算方案、制造方法、工艺流程、计算机软件、数据库、实验结果、技术数据、图纸、样品、样机、模型、模具、说明书、操作手册、技术文档、设计商业秘密的业务函电等一切有关的信息。

第二条 对秘密信息的保密

乙方承诺，严格保守自己在为甲方工作期间所获得有关甲方及甲方项目的一切秘密信息。

乙方保证除非为了甲方项目的工作需要交流此种秘密信息外，未经甲方事先书面许可，不以任何方式，无论口头、书面，还是磁盘、通信网络等介质向任何其他方，包括个人、企业、商社、其他经济组织等泄露秘密信息。

第三条 保密期限

聘用合同期内即解除聘用合同后的____年内。

第四条 保密费的数额及支付方式

甲方对乙方的技术成果给予的奖励，奖金中含有保密费，其奖金和保密费的数额，视技术成果的作用及其创造的经济效益而定。

第五条 违约责任

如果乙方违反本协议的规定，应赔偿甲方全部损失。赔偿范围包括但不限于甲方的名誉损失、直接损失和可得利益的损失，以及调查费用和诉讼费用、律师费用。

第六条 协议的生效与效力

1、本协议自甲、乙双方签字之日起生效。

2、双方就履行中产生的任何争议，应通过友好协商解决，协商不成，任何一方有权向人民法院提起诉讼。

3、本协议一式二份，甲、乙双方各执一份，具有同等法律效力。

甲方： 乙方：

年 月 日 年 月 日

附 录 D
（资料性附录）
商业秘密突发事件应急预案

为建立健全企业商业秘密保护工作机制，提高企业应对商业秘密涉密突发事件的能力，保障企业各项生产、经营、科研活动正常展开，特制定本方案。本方案适用于企业以及所属的各部门。

一、制定商业秘密突发事件应急预案的目的

及时掌握涉密突发事件，及时协调各部门及相关的政府机构，将涉密突发事件的危害降到最低。

二、应急处置基本原则

本预案应急处置遵循“依靠技术、加强管理、预防为主、快速响应”的总原则。另外应做到以下几点：

1、统一领导、分工协作

在企业商业秘密保护委员会统一领导下，明确各部门及相关人员职责，督促相关部门遵照“统一领导、归口负责、综合协调、各司其职”的原则，协同配合，有效地处置突发事件和应急情况。

2、明确责任，依法规范

各部门要按照“属地管理、分级响应、及时发现、及时报告、及时救治、及时控制”的要求，依法对涉密突发事件进行防范、监测、预警、报告、响应、指挥、协调和控制。

3、统筹安排、协调配合

企业商业秘密保护委员会统筹安排各部门应急工作任务，充分利用企业现有的技术力量和监控设备等。各部门应在明确职责的基础上，加强协调，密切配合。

4、防范为主、加强监控

贯彻预防为主的思想，树立常备不懈的观念，在企业内宣传普及保护商业秘密的意识和知识，做好应对涉密突发事件的思想准备、机制准备和硬件准备。

5、快速处理，降低损失

突发涉密事件时，能够及时发现和预警，准确判断并及时采取有效措施，迅速控制涉密事件的程度和范围，并在第一时间联系政府、公安、市场监管等相关部门，尽可能减少突发事件对我企业的负面影响。

三、涉密事件类型

1、网络入侵事件：通过非授权方式侵入企业信息系统，对相关信息资产进行非授权监听、调用、篡改、销毁等，造成企业管理、经营的负面影响和重大损失。

2、计算机病毒破坏事件：病毒、非预期程序代码植入企业信息系统，造成商业秘密泄露。

3、重要存储介质失窃事件：存储有企业重要数据、各级商业秘密等信息的各类存储介质的遗失、失窃等，如纸质文件资料、硬盘、U盘、光盘等。

4、人员泄密事件：企业原掌握商业秘密的人员因离职或跳槽等原因泄露我企业商业秘密。

四、应急指挥机构及职责

组长：XXX

职责：统筹安排各部门任务

副组长：XXX

职责：协助组长

成员：XXX、XXX、XXX

XXX履行应急值守和综合协调职责；XXX联系政府、公安、市场监管等相关部门；XXX对涉密事件进行调查，并组织评估。

联系电话：XXXXXXXXXXXXX

五、应急响应与处置

涉及企业绝密级商业秘密的事件警报为一级警报，现场发现人员应立即上报部门负责人，部门负责人立即上报给应急指挥小组组长。

涉及企业机密级商业秘密的事件警报为二级警报，现场发现人员应在30分钟内上报部门负责人，部门负责人立即上报给应急指挥小组组长。

涉及企业秘密级商业秘密的事件警报为三级警报，现场发现人员应在60分钟内上报部门负责人，部门负责人在30分钟内上报给应急指挥小组组长。

涉密突发事件报告分为首报、续报、终报。

首报内容应包括：涉密事件发生的时间、地点、等级；续报内容应包括：涉密事件的范围、趋势、处置情况、请求事项；终报内容应包括：涉密事件基本情况，原因分析、处置过程、影响评估、责任划分与处理、教训和预防措施。