企业商业秘密保护管理制度

Management Specification for Protection of Trade Secrets of Enterprises

目　　次

企业商业秘密保护管理制度

1 范围

本文件规定了本单位商业秘密保护管理的一般要求、涉密节点管理、涉密人员管理、涉密载体管理、涉密区域管理、涉密活动管理、维权救济管理和监督检查管理等内容。

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。

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。

3.2

涉密人员 secret-related personnel

根据工作职责或者保密协议有权接触、使用、掌握商业秘密的企业员工或其他人。

3.3

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。

3.4

涉密区域 secret-related area

可以接触到商业秘密信息的一切场所，包括但不限于企业园区、厂房、车间、实验室、办公室、保密室、档案室、机房、用户现场等。

4 一般要求

4.1 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”的原则。

4.2 企业应全方位构建以最高管理者为第一责任人，领导责任、监管责任、部门责任一体贯穿的商业秘密保护管理体系。

4.3 企业董事会等决策管理层应履行商业秘密保护的领导责任，其职责包括但不限于:

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制度情况；
d) 做好企业商业秘密保护管理制度体系的评价与改进。

4.4 企业商业秘密保护部门/岗位人员，履行商业秘密保护的监管责任，其职责包括但不限于：

a）执行企业商业秘密保护领导机构的决策决议；
b）研究制定企业商业秘密保护管理制度；
c）形成企业商业秘密保密事项清单并动态更新；
d）组织对企业员工进行商业秘密保护教育培训；
e）指导、监督业务部门制定实施生产、经营相关的商业秘密保护方案；
f）组织企业内部商业秘密风险隐患排查并落实专项整治；
g）做好泄密事件的应急处理，配合有关部门完成商业秘密侵权事件的调查举证。

4.5 企业研发、生产、销售、人事、财务等业务部门应履行商业秘密保护的部门责任，其职责包括但不限于：

a) 梳理本部门保密事项清单并动态更新；
b) 全员严格遵守企业商业秘密保护规章制度、落实保密岗位责任；
c) 建立并执行分析预警、自查评估等制度；
d) 及时发现上报商业秘密泄密隐患、侵权线索等。

4.6 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、集成电路布图等系统布局，立体保护。

4.7 企业宜加强商业秘密前置保护，可应用区块链等商业秘密存证平台，实施预先存证保护措施。

5 涉密节点管理

5.1 定密

5.1.1 企业应对商业秘密进行核查和评估，其表现形式、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；
c) 其他的具有价值的商业信息。

5.1.2 对企业的商业秘密进行核查和评估时应考虑以下一般因素：

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的未来价值；
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。

5.1.3 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。

5.1.4 可对技术秘密进行科技查新，确认其不为公众所知悉。

5.1.5 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。

5.1.6 对核查和评估后已经确定的商业秘密，可通过电子数据存证或公证等证据保全方式实现对商业秘密权属的初步确认。

5.1.7 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等多个保护等级，实行定期复评、动态调整。

5.1.8 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，企业应对商业秘密和国家秘密进行分类管理。

5.2 隐密

5.2.1 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。

5.2.2 可采取的隐密方式为：

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。

5.3 解密

5.3.1 商业秘密的解密应满足下列要求：

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

5.3.2 可采取的解密方式为：

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

5.4 销密

5.4.1 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。

5.4.2 可采取的销毁方式为：

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） 含有核心秘密的电子信息载体应做销毁处理；
d） 其他合适的方式。

5.4.3 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。

6 涉密人员管理

6.1 入职管理

6.1.1 应对涉密岗位的拟入职员工进行背景调查。必要时，可要求拟入职员工做出在企业任职期间不侵犯前雇主的商业秘密、不违反与前雇主签订的竞业限制协议等的承诺。

6.1.2 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。

6.1.3 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。

6.1.4 对高级管理人员、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。

6.1.5 应对新入职涉密岗位的人员进行商业秘密保护培训，在培训结束后宜进行考核，保存相关考核材料。

6.2 在职管理

6.2.1 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。

6.2.2 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等。

6.2.3 将商业秘密保护培训列入企业年度培训计划，开展全员保密知识普及并组织不同涉密岗位人员分别参加有针对性的保密教育培训，保存培训记录。

6.3 离职管理

6.3.1 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。

6.3.2 提醒离职员工主动移交一切涉密载体和物品，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。

6.3.3 应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。

6.3.4 应开展离职检查，检查内容包括：

a） 工作电脑数据是否完整；
b） 工作账户是否有异常操作，如异常查询、下载、拷贝、修改、删除等；
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。

6.3.5 应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，并应及时掌握离职员工在竞业限制期限内的任职去向。

7 涉密载体管理

7.1 涉密文件资料

7.1.1 应有密级、保护期限等标识，实行登记管理、归档存放。

7.1.2 按权限使用，查阅、借阅、续借应履行登记手续。

7.1.3 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。

7.1.4 新闻发布、论文发表、专利申请等信息发布和公开前，由商业秘密保护专门机构对信息进行审核。

7.2 涉密电子信息

7.2.1 存储

7.2.1.1 涉密数据应存储于企业授权的存储设备和应用系统或云存储空间。核心秘密、重要秘密等级的数据应采用加密方式存储，并定期备份后妥善保存。

7.2.1.2 涉密电子信息物理载体的采购、维护应进行归档登记，并选用安全稳定、运转正常的电脑、手机、硬盘等存储介质。存储介质送外维修前应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。

7.2.1.3 涉密电子信息存储系统应定期进行安全检查，发现系统漏洞及时修补。宜安装防恶意代码软件，并及时更新软件版本和恶意代码库。

7.2.1.4 涉密电子信息使用云储存时，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。

7.2.2 权限

7.2.2.1 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。

7.2.2.2 权限到期、人员转岗、项目或事项变更时应重新授权。

7.2.2.3 人员离职时应回收相应权限。

7.2.3 口令

7.2.3.1 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。

7.2.3.2 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。

7.2.3.3 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。

7.2.4 流转

7.2.4.1 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。

7.2.4.2 必要时，应使内部局域网与互联网隔离，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。

7.2.4.3 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。

7.2.4.4 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。

7.2.4.5 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。

7.2.4.6 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。

8 涉密区域管理

8.1 涉密重点区域应予明确划定标示，包括但不限于：

a) 研发设计、信息管理、财务、人力资源部门核心区域；
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。

8.2 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) 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；
b) 进出口处应安装视频监控设施和报警装置；
c) 限制使用具有录音、摄像、拍照、信息存储等功能的设备；
d) 必要时采取网络隔离阻断等。

8.3 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。

8.4 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。

9 涉密活动管理

9.1 在商务合作、共同开发、委托加工等商务活动中，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，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。

9.2 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、资料控制发放范围，做好发放登记，及时收回清点。
e） 通过拍照、摄像、签名等方式，做好记录等。

9.3 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。

9.4 接受外部单位开展的执法、检查等活动前，如须进入涉密区域、接触涉密信息等，应提示其履行保密义务。

10 维权救济管理

10.1 侵权评估

发现商业秘密涉嫌被侵权或被控侵犯商业秘密时：

a） 应及时向管理部门上报；
b） 评估所涉商业秘密性质、类别；
c） 评估所涉商业秘密的范围及具体内容；
d） 评估所涉商业秘密的侵权方式；
e） 评估商业秘密侵权相关主体的情况；
f） 评估商业秘密侵权对企业可能造成的损害或影响。

10.2 维权方案

10.2.1 维权方案内容包括但不限于：

a） 成立工作专班，明确任务分工；

b） 维权目标、维权途径；
c） 维权措施，取证策略；
d） 时间计划及重要节点；
e） 是否聘请律师等第三方专业团队；
f） 资金预算等。

10.2.2 维权方案可根据案件进展进行动态调整。

10.3 取证固证

10.3.1 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） 侵权嫌疑人的情况；
d） 侵权嫌疑人接触或有可能接触本企业商业秘密；
e） 侵权嫌疑人采取不正当手段。

10.3.2 企业被控侵犯他人商业秘密时，应及时收集相关证据，包括：

a） 所指称的商业秘密不符合法定构成要件，证据包括：
   1） 商业秘密已为公众所知悉，
   2） 商业秘密不能带来经济价值，
   3） 商业秘密未被采取保密措施；
b） 企业实施的技术与所指称的商业秘密不同；
c） 他人不是所指称商业秘密的合法权利主体；
d） 企业无机会接触所指称的商业秘密。

10.4 维权路径

10.4.1 根据证据收集情况，企业可依法采取下列方式进行维权：

a） 向涉嫌侵权单位及个人发出警示函、律师函等，开展自主协商；
b） 向行政主管部门举报投诉；
c） 申请劳动仲裁或商事仲裁；
d） 向公安机关控告；
e） 向人民法院提起民事诉讼；
f） 向人民检察院提起商业秘密诉讼活动法律监督等。

10.4.2 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。

11 监督检查管理

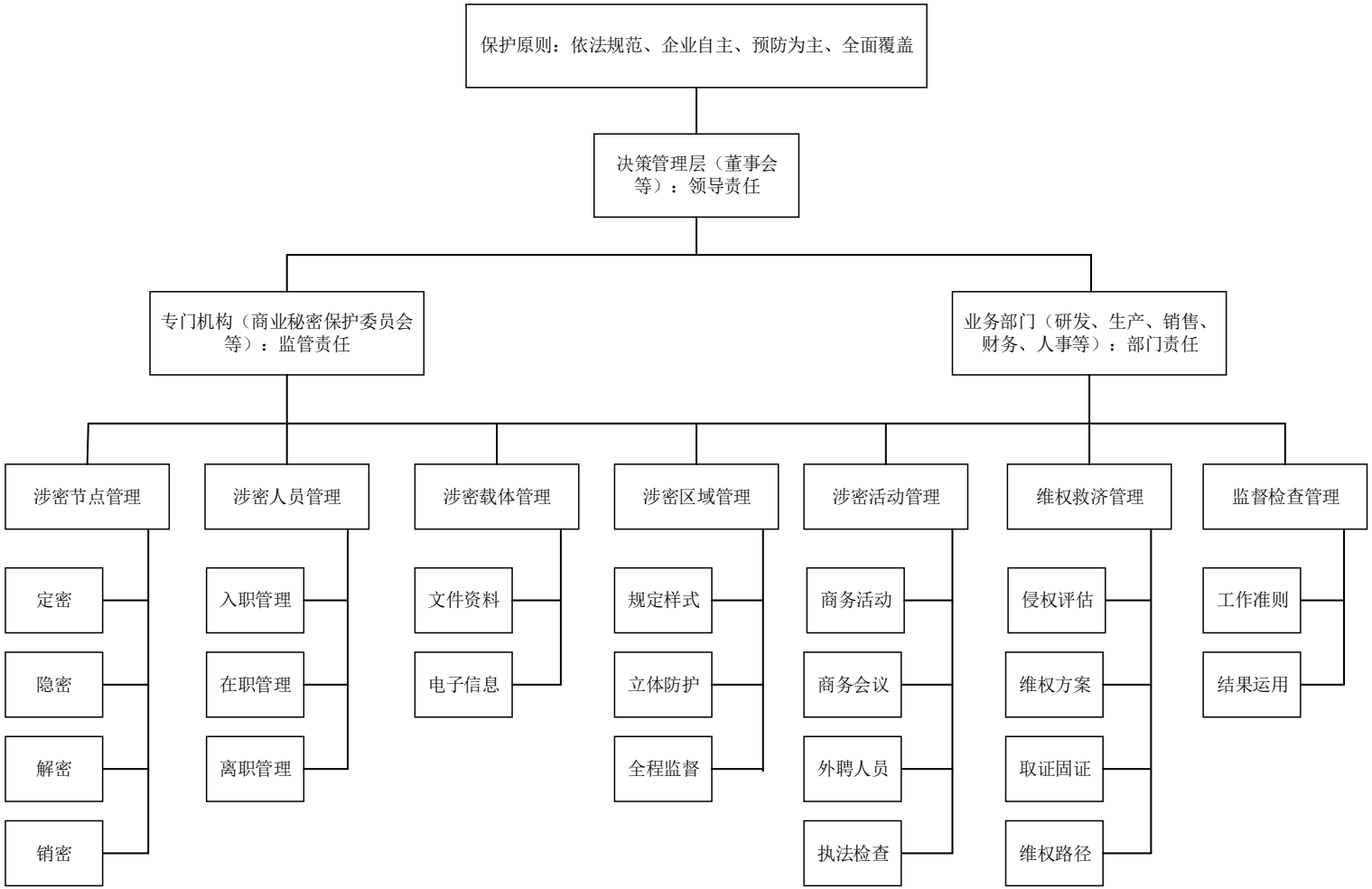
11.1 企业应建立并执行监督检查准则，主要包括：

a） 监督检查的内容和方法；
b） 监督检查的各级职责和权限；
c） 执行监督检查的频次与时限。

11.2 监督检查的内容包括企业商业秘密保护管理各项制度的实施情况、奖惩落实情况等。

11.3 监督检查的方法包括但不限于随机临检、抽查文档、人员询问、电子监控等。

11.4 企业应强化监督检查结果运用，建立完善商业秘密保护奖惩激励、应急处置等日常工作机制。


保护原则：依法规范、企业自主、预防为主、全面覆盖
决策管理层（董事会等）：领导责任
专门机构（商业秘密保护委员会等）：监管责任
业务部门（研发、生产、销售、财务、人事等）：部门责任
涉密节点管理
涉密人员管理
涉密载体管理
涉密区域管理
涉密活动管理
维权救济管理
监督检查管理
定密
隐密
解密
销密
入职管理
在职管理
离职管理
文件资料
电子信息
规定样式
立体防护
全程监督
商务活动
商务会议
外聘人员
执法检查
侵权评估
维权方案
取证固证
维权路径
工作准则
结果运用