ICS 03.140
CCS A 00

团　　体　　标　　准

T/PPAC 701—2021

企业商业秘密管理规范

Enterprise trade secret management

2021-12-31 发布　　2022-01-01 实施

中国专利保护协会　　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。

本文件由中国专利保护协会提出。

本文件起草单位：中国专利保护协会、中知（北京）认证有限公司、中国冶金科工集团有限公司、中国标准化研究院、北京黑马企服科技有限公司。

本文件主要起草人：马维野、马鸿雅、王文静、余平、宋巧丽、翟晨阳、郭伟红、张陆军、张永华、黄武双、刘海波、宋健、姚兵兵、张雪红、王丽娟、刘作信、邢文超、王伟、徐可欣、陈蓓艳、杨昕、岳高峰、杨洋、王健琳、程文武。

引　言

0.1　总则

知识产权作为经济发展的重要资源和竞争力的核心要素，在企业竞争中的作用日渐突出。商业秘密是企业重要的知识产权之一，也是企业的核心竞争力。本文件旨在指导企业依据法律法规和自身发展战略目标，建立并完善商业秘密管理体系，更好地保护商业秘密，降低商业秘密泄露的风险，提升竞争优势；合理地防控商业秘密侵权的风险，提升合规管理水平，营造企业尊重知识产权的良好氛围；综合运用知识产权，实现无形资产的保值和增值。

0.2　商业秘密管理原则

企业在实施商业秘密管理时应遵循下列原则：

a）　最高层管理原则：商业秘密是企业的核心竞争力，是企业最重要的核心资产；最高管理者作为商业秘密管理的第一责任人，支持和参与是商业秘密管理的关键；

b）　全流程管理原则：商业秘密涉及企业的方方面面，企业应将商业秘密的管理融入企业的研发、设计、采购、生产、施工建设、商务合作、对外交流、信息披露、销售、设备维修、工艺改造、人事、财务、信息化、法务等业务过程；

c）　平衡管理原则：企业应通过分类分级、信息化等管理手段在商业秘密安全、管理效率与管理成本之间寻求平衡，在保证商业秘密安全的前提下提高管理效率、降低管理成本。

0.3　过程方法

0.3.1　总则

本文件倡导在建立、实施商业秘密管理体系以及提高其有效性时采用过程方法，应用过程方法可以：

a）　理解并持续满足要求；

b）　获得有效的过程绩效；

c）　在评价数据和信息的基础上改进过程。

具体要求见4.4。

0.3.2　PDCA循环

本文件倡导在过程中使用PDCA循环，应用PDCA循环有助于快速适应环境和相关方需求的变化；有助于管理水平的阶梯式提升；有助于商业秘密管理体系的不断完善。本文件第4章～第11章内容在PDCA循环中的应用如图1所示。

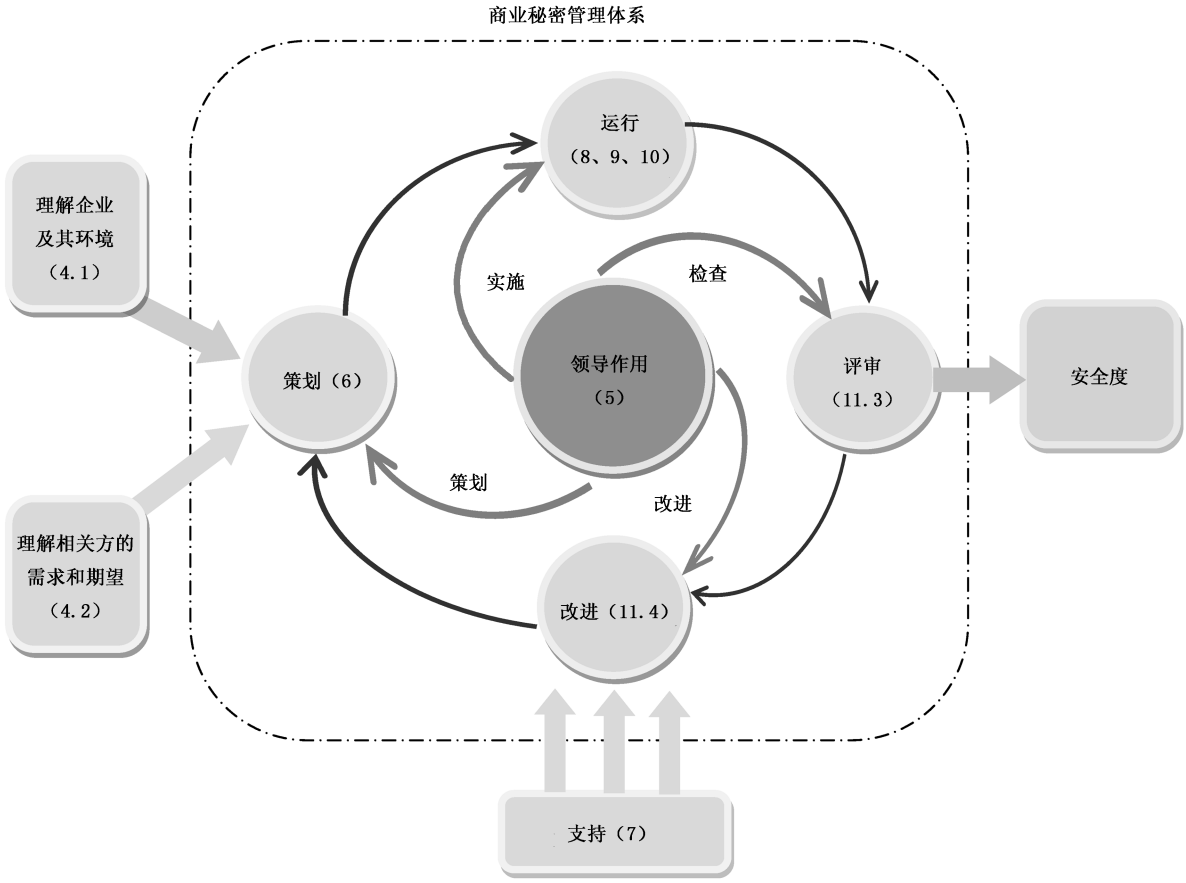

图 1　本文件基本结构的 PDCA 循环

0.4　与其他管理体系的关系

0.4.1　总则

本文件采用 ISO/IEC 管理体系的高层体系结构（HLS），以确保与其他管理体系标准的协调一致性。

0.4.2　国家秘密管理

国家秘密和商业秘密可能存在交叉，企业应在严格遵循国家秘密相关法律法规规定的同时，遵守本文件的要求，实现利益最大化。本文件为统筹协调国家秘密和商业秘密提供了参考。

0.4.3　知识管理

GB/T 34061.1 中知识保护的环节要求组织应注重组织内部知识的安全保密，避免因人员的流动、合作伙伴、供应商等因素导致的知识流失与损失。本文件为通过商业秘密保护知识提供了依据。

0.4.4　信息安全管理

商业秘密管理中涉及大量的信息安全管理，企业可依据 GB/T 22080 中提到的技术手段实施商业秘密信息的管理。

0.4.5 知识产权管理

商业秘密管理是企业知识产权管理的重要组成部分，本文件为 GB/T 29490 商业秘密管理的补充和完善，但本文件仍保持体系的相对完整性。

企业在实施知识管理、信息安全管理、知识产权管理等相关体系时，可参考本文件完善相关的管理措施。

企业商业秘密管理规范

1 范围

本文件规定了商业秘密管理的基本原则、策划、实施、检查及改进。

本文件适用于有下列目标的企业：

a） 建立并完善企业商业秘密管理体系，降低泄密风险和侵权风险；

b） 获取第三方专业机构对本企业商业秘密管理体系的评价；

c） 利用本文件为其他企业提供服务。

具有商业秘密管理需求的其他组织可参照本文件执行。

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

技术信息 technical information

与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、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。

注：《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》第一条。

3.2

经营信息 commercial information

与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息。

注 1：客户信息包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

注 2：《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》第一条。

3.3

商业秘密 trade secret

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 1：《中华人民共和国反不正当竞争法》第九条。

注 2：权利人包括商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人（《中华人民共和国刑法》第二百一十九条）。

3.4

管理体系 management system

组织建立方针和目标以及实现这些目标的过程的相互关联或相互作用的一组要素。

注 1：一个管理体系可以针对单一的领域或几个领域，如质量管理、财务管理或环境管理。

注 2：管理体系要素规定了组织的结构、岗位和职责、策划、运行、方针、惯例、规则、理念、目标，以及实现这些目标的过程。

注 3：管理体系的范围可能包括整个组织，组织中可被明确识别的职能或可被明确识别的部门，以及跨组织的单一职能或多个职能。

[来源：GB/T 19000—2016，3.5.3]

3.5

商业秘密管理体系　trade secret management system

建立商业秘密方针和目标并实现这些目标的体系。

3.6

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。

注：涉密人员一般包括涉密管理人员和商业秘密接触人员。

3.7

涉密载体　secret-related carrier

以文字、数据、符号、图形、实物、视频和音频等形式记载和存储商业秘密的纸介质、光介质、电磁介质等各类物品。

注 1：纸介质是指传统的纸质涉密文件资料、书刊、图纸等。

注 2：光介质是指利用激光原理写入和读取商业秘密的存储介质，包括 CD、VCD、DVD 等各类光盘。

注 3：电磁介质包括电子介质和磁介质两种，如各类闪存盘、硬磁盘、软磁盘、磁带等。

3.8

涉密设备　secret-related device

生成、存储、处理商业秘密的设备以及通过观察或者测试、分析手段能够获得商业秘密的设备或产品。

3.9

涉密区域　secret-related area

可以接触到商业秘密信息的一切场所。

注：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。

3.10

安全度　safety degree

商业秘密安全与否的客观程度。

3.11

成文信息　documented information

组织需要控制和保持的信息及其载体。

注 1：成文信息可以任何格式和载体存在，并可来自任何来源。

注 2：成文信息可涉及：

——管理体系，包括相关过程；

——为组织运行产生的信息（一组文件）；

——结果实现的证据（记录）。

[来源：GB/T 19000—2016，3.8.6]

3.12

显性知识　explicit knowledge

以文字、符号、图形等方式表达的知识。

[来源：GB/T 23703.2—2010，2.3]

3.13

隐性知识　tacit knowledge

未以文字、符号、图形等方式表达的知识，存在于人的大脑中。

[来源：GB/T 23703.2—2010，2.4]

4 企业环境

4.1 理解企业及其环境

4.1.1 外部环境

企业应收集并识别分析来自国内外的法律法规、技术、竞争、市场、文化、社会和经济环境等外部环境的相关信息。

企业应定期对外部环境的相关信息进行监测和评审。

4.1.2 内部因素

企业应收集并识别分析企业价值观、文化、知识和绩效等内部因素的相关信息，最终确定影响其实现商业秘密管理体系的因素。

企业应定期对内部因素的相关信息进行监测和评审。

4.2 理解相关方的需求和期望

由于相关方的需求和期望影响或潜在影响企业的商业秘密管理责任和能力，因此，企业应确定：

a) 商业秘密管理体系相关方包括但不限于：顾客、供方、合作伙伴、员工的前雇主、监管部门等；

b) 商业秘密管理体系相关方的要求包括但不限于：商业秘密的定义、商业秘密的诉讼要求、合同中关于保守商业秘密的约定、员工与前雇主签订的保密协议等。

企业应监测和评审这些相关方的信息及其相关要求。

4.3 确定商业秘密管理体系的范围

企业应确定商业秘密管理体系的边界和适用性，以确定其范围。在确定范围时，应考虑：

a) 4.1 中提及的各种外部环境和内部因素；

b) 4.2 中提及的相关方的要求；

c) 企业商业秘密保护的要求。

企业的商业秘密管理体系范围应作为成文信息，可获得并得到保持。该范围应描述企业所涉及的商业秘密的种类。如果本文件的全部要求适用于企业确定的商业秘密管理体系的范围，企业应实施本文件的全部要求。如果企业确定本文件的某些要求不适用于其商业秘密管理体系范围，应说明理由。

只有当所确定的不适用的要求不影响企业的商业秘密管理能力或责任时，方可声称符合本文件的要求。

4.4 商业秘密管理体系及其过程

4.4.1 企业应按照本文件的要求，建立、实施、保持和持续改进商业秘密管理体系，包括所需过程及其相互作用。

企业应确定商业秘密管理体系所需的过程及其在整个企业中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；

c) 确定和应用所需的准则和方法（包括监测、评价和相关绩效指标），以确保这些过程的有效运行和控制；

d） 确定这些过程所需的资源并确保其可获得；
e） 分配这些过程的职责和权限；
f） 按照 6.1 的要求应对风险和机遇；
g） 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
h） 改进过程和商业秘密管理体系。

4.4.2 在必要的范围和程度上，企业应：
a） 保持成文信息以支持过程运行；
b） 保留成文信息以确信其过程按策划进行。

5 领导作用

5.1 领导作用及承诺

最高管理者应通过以下方面，证实其对商业秘密管理体系的领导作用和承诺：
a） 确保制定商业秘密管理体系的方针和目标，并与企业环境相适应，与战略方向相一致；
b） 确保商业秘密管理体系融入企业的相关业务全过程，实现安全与管理效率、管理成本的平衡；
c） 确保商业秘密管理体系运行所需的资源；
d） 确保通过 PDCA 循环实现商业秘密管理体系的持续改进；
e） 支持其他相关管理者在其职责范围内发挥领导作用。

5.2 方针

最高管理者应制定、保持商业秘密方针，并确保在企业内得到沟通、理解和应用。商业秘密方针应：
a） 符合企业的宗旨和环境，同企业的研发战略、知识产权战略相协调，并支持企业的总体战略；
b） 为建立商业秘密管理目标提供框架；
c） 包含适用性和持续改进的承诺；
d） 保持成文信息。

5.3 岗位、职责及权限

最高管理者应确保企业设置商业秘密管理相关岗位，明确岗位职责和权限，并确保全体员工知悉和理解。

最高管理者应分配职责和权限，以：
a） 确保商业秘密管理体系符合本文件的要求；
b） 确保全体员工能够理解商业秘密管理和商业秘密管理体系有效运行的重要性；
c） 促进使用过程方法确保各过程获得其预期输出；
d） 确保商业秘密管理体系实现其预期结果；
e） 报告商业秘密管理体系的绩效，提出改进建议；
f） 在策划和实施商业秘密管理体系变更时，应保持其完整性。

6 策划

6.1 应对风险和机遇的措施

在策划商业秘密管理体系时，企业应考虑到 4.1 所提及的因素和 4.2 所提及的要求，确定需要应对

的风险和机遇，并策划：

a） 应对这些风险和机遇的措施；

b） 确保商业秘密管理体系能够实现其预期结果；

c） 增强有利影响，预防或减少不利影响；

d） 如何在商业秘密管理体系过程中整合、实施这些措施并评价措施的有效性（见 4.4）；

e） 实现持续改进。

注 1：应对风险可选择规避风险，为寻求机遇承担风险、消除风险源、改变风险的可能性或后果、分担风险或通过信息充分的决策而保留风险。

注 2：机遇可能导致采用新实践、推出新产品、开辟新市场、赢得新顾客、建立合作伙伴关系、利用新技术等，以满足企业或其相关方的需求。

6.2 管理目标及其实现的策划

企业应根据相关职能、层次和商业秘密管理体系所需的过程建立商业秘密管理目标。企业应策划所需资源、职责、工作内容、监督检查、评审等，实现管理目标。管理目标应：

a） 与商业秘密方针保持一致，可包括长期目标和中、短期目标；

b） 可考核、可评价；

c） 予以沟通，确保全员能够理解商业秘密管理的重要性及其管理目标；

d） 予以监督检查、考核和评价；

e） 适时更新。

6.3 变更的策划

当企业确定需要对商业秘密管理体系进行变更时，变更应按所策划的方式实施（见 4.4）。并考虑：变更目的及其潜在后果；商业秘密管理体系的完整性；资源的可获得性；职责和权限的分配或再分配。

7 支持

7.1 资源

企业应提供建立、实施、保持和持续改进商业秘密管理体系所需的资源。包括：

a） 企业应确定并配备所需的人员，以有效实施商业秘密管理体系，并运行和控制其过程；

b） 企业应确定、提供并维护所需的基础设施，以支撑商业秘密管理过程的运行；

c） 企业应确定、提供必要的经费，以保障商业秘密管理过程的运行。

注：基础设施可包括：建筑物和相关设施；设备，包括硬件和软件；信息系统和技术手段等。

7.2 能力

企业应：

a） 确定影响商业秘密管理体系绩效和有效性的人员所需具备的能力；

b） 通过法律法规、保密责任、保密意识、保密措施等教育培训或招聘有经验的人员，确保人员能够胜任其工作；

c） 适用时，通过对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员等措施获得所需的能力，并评价措施的有效性；

d） 保留适当的成文信息，作为人员能力的证据。

7.3 意识

企业应确保商业秘密管理体系相关人员理解：

a） 商业秘密方针和管理目标；

b） 其对商业秘密管理体系有效性的贡献，包括改进绩效的益处；

c） 不符合商业秘密管理体系要求的后果。

7.4 沟通

企业应建立有效的沟通交流方式，确保商业秘密管理体系内部不同层级之间的需求得到理解，并及时获得反馈。

企业应建立沟通机制，确保与商业秘密相关的外部沟通。

7.5 成文信息

7.5.1 总则

成文信息是商业秘密管理体系重要的组成部分。商业秘密管理体系成文信息包括：本文件要求的成文信息；企业所确定的、为确保商业秘密管理体系有效性所需的成文信息。

由于不同的企业其规模、活动、过程、产品和服务的类型不同，过程及其相互作用的复杂程度不同以及人员的能力不同，商业秘密管理体系成文信息的多少与详略程度可以不同。

7.5.2 创建和更新

在创建和更新成文信息时，企业应：

a） 进行合理的标识和说明（如标题、日期、作者、索引编号）；

b） 采取合适的形式（如语言、软件版本、图表）和载体（如纸质的、电子的）；

c） 适当地进行评审、批准，以确保适宜性和充分性。

7.5.3 成文信息的控制

企业应对商业秘密管理体系和本文件所要求的成文信息进行妥善保护，防止泄密、不当使用或缺失，并确保在需要的场合和时机可获得并适用。

企业应对成文信息进行分发、使用、存储和防护，并对版本的更改进行控制，确保成文信息的保留和处置。

对于企业确定的策划和运行商业秘密管理体系所必需的来自外部的成文信息，企业应进行适当识别，并予以控制。

对所保留的、作为符合性证据的成文信息应予以保护，防止未经评审、批准的更改。

8 商业秘密的确定

8.1 总则

企业应定期或不定期组织商业秘密确定工作，包括：

a） 确定商业秘密的范围、保密事项等，并形成商业秘密清单；

b） 对商业秘密进行分类分级；

c） 对商业秘密的成文信息进行储存保管；

d） 对商业秘密清单进行适时更新。

8.2 确定商业秘密

8.2.1 商业秘密遴选

企业应：

a） 定期或不定期对经营活动中产生的战略规划、管理方法、商业模式、改制上市、并购重组、产权交易、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息，以及设计、程序、产品配方、制作工艺、制作方法、技术诀窍等技术信息进行分析，遴选出商业秘密；

b） 特别是在重大经营活动、项目的重要节点，应及时开展商业秘密遴选等工作。

8.2.2 分类分级

企业在对商业秘密进行分类分级时，应考虑其秘密性和价值性，并保留成文信息：

a） 商业秘密应是不为所属领域相关人员普遍知悉和容易获得的信息；

b） 考虑商业秘密与企业主营业务的关联程度，泄露后对于企业的影响以及在现阶段的市场地位、技术先进性及潜在的发展前景等，评估其经济价值；可将研发成本、合同价格或市场前景分析等信息作为评估其经济价值的参考。

8.2.3 确定保护形式

企业根据商业秘密的分类分级，应制定不同要求：

a） 对商业秘密是否属于国家秘密进行判断，如商业秘密属于国家秘密的，应按照国家保密相关法律法规进行管理；

b） 如既属于国家秘密又属于商业秘密的，则应同时符合国家秘密管理和本文件的要求；

c） 企业应对遴选出的商业秘密进行评估，确定合适的保护形式，如：进行防卫性公开、申请专利、作为商业秘密等，需要通过商业秘密保护的隐性知识应及时转化为显性知识。

8.3 确定保密事项

8.3.1 密级划分

根据商业秘密的秘密性和价值性，企业可将密级划分为：

a） 核心商密，泄露会使企业的主营业务及核心利益遭受特别严重的损害；

b） 重要商密，泄露会使企业利益遭受严重损害；

c） 一般商密，泄露会使企业利益遭受损害。

8.3.2 确定保密期限

企业可根据商业秘密的密级划分以及商业秘密生命周期、技术成熟程度、潜在价值、市场需求等，确定商业秘密保密期限。可以预见时限的以年、月、日计，不可以预见时限的应定为“长期”或者“公布前”。

8.3.3 确定接触范围

企业应根据商业秘密的内容和密级，确定商业秘密的主责部门与接触范围。

企业应保留接触范围的成文信息。

8.3.4 确定流转要求

企业应根据商业秘密的内容和密级确定商业秘密的流转要求；通过信息系统或者会议等形式发布时，应采取签字或者数字化身份认证等方式记录接触范围。

企业应保留商业秘密流转的成文信息。

8.3.5 存证

企业应根据涉密载体管理条件、商业秘密的密级与载体情况确定合适的存证方式：

a) 对于商业秘密所涉及的文件，企业应通过编校审等书面签字审核流程或带有时间戳的电子审核流程，使之成为受控文件；

b) 企业可将必要且适当的涉密载体委托第三方机构进行存证；第三方机构应为具有一定社会公信力的、独立的、经相关司法机关认可的法人主体；商业秘密存证的信息载体可以是报告、论文、图纸、磁带、磁盘等信息化载体，也可以是样品、样机等物化载体。

8.3.6 商业秘密清单

企业应形成商业秘密清单，内容可包括商业秘密主题、密级、保密期限、主责部门、接触范围、流转要求、保存方式、存证方式等。

8.4 更新与解密

商业秘密的更新与解密应满足下列要求：

a) 当内外部环境发生变化时，企业应对确定商业秘密的依据及商业秘密的范围进行考察，确保商业秘密信息范围和密级及时更新，并及时对商业秘密清单予以更新；

b) 企业应定期对其商业秘密进行评估，考察商业秘密信息是否需要解密；当出现商业秘密被公开，或失去保护价值等情况时，可将商业秘密解密，并对商业秘密清单予以更新；

c) 国家秘密到期解密时，企业应对其进行评估确定是否继续作为商业秘密进行管理；

d) 商业秘密解密时，企业应对其进行评估确定是否以其他形式的知识产权进行保护。

9 商业秘密的管理

9.1 总则

企业应建立涉密人员、涉密载体、涉密设备、涉密区域的管理要求，并按照要求开展商业秘密管理工作。

对于重要的项目，可以建立针对特定项目的管理制度，与重要岗位人员签署特定的保密协议。

企业应保持商业秘密管理的成文信息。

9.2 涉密人员管理

9.2.1 入职管理

9.2.1.1 招聘

企业人员招聘应满足下列要求：

a) 根据商业秘密清单确定拟招聘的岗位是否属于涉密岗位；

b） 应对涉密岗位的应聘人员进行保密事项提醒，告知其有保护本企业商业秘密的义务，并提醒其不得泄露前雇主的商业秘密；必要时，可要求其作出知悉承诺或签署保密承诺书；

c） 对涉密岗位的拟入职员工进行背景调查，以避免因新员工入职带来法律风险；必要时要求其作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；

d） 企业应保留涉密事项提醒、背景调查的成文信息。

9.2.1.2 保密协议

企业应与新入职员工签署保密协议，约定保密范围、双方的权利和义务、违约责任等。

企业应保留保密协议的成文信息。

9.2.1.3 竞业限制协议

企业应与新入职的高级管理人员、高级技术人员和其他知悉核心、重要商业秘密的人员签署竞业限制协议，并约定竞业限制的范围、地域、生效条件、期限、违约责任、经济补偿等。

企业应保留竞业限制协议的成文信息。

9.2.1.4 保密培训

企业应对新入职员工进行保密培训，以确保其：

a） 理解商业秘密权利、义务，建立保密意识；

b） 理解企业商业秘密管理相关规定；

c） 理解其岗位的保密责任。

企业应保留保密培训的成文信息。

9.2.2 在职管理

9.2.2.1 日常管理

企业应根据涉密岗位及各部门的工作内容建立涉密人员清单，并定期更新。

企业应根据商业秘密清单、接触商业秘密的情况等动态更新涉密岗位及涉密人员清单，完善制度，做好日常保密培训。

企业应定期梳理高级管理人员、高级技术人员和其他知悉核心、重要商业秘密的人员，确定是否补签竞业限制协议。

9.2.2.2 保密承诺

企业应根据员工在工作中所接触的商业秘密具体内容，定期或不定期要求其签署保密承诺书。

企业应保留保密承诺的成文信息。

9.2.2.3 保密培训

企业应定期进行保密培训，以确保员工：

a） 理解企业商业秘密管理的重要性、制度、程序；

b） 知悉其保护商业秘密的权利和义务；

c） 理解内部、外部人员的正当、不正当行为可能带来的泄密风险和处理方式。

企业应保留保密培训的成文信息。

注：保密培训可包括法律法规培训、保密责任培训、保密意识培训、保密措施培训等。

9.2.2.4 岗位变动

企业应督促岗位变动员工做好保密材料交接工作，对员工重新划分涉密类别与层级，及时做好涉密接触权限的调整，并做好脱密期管理工作。

9.2.3 离职管理

企业应做好涉密人员的离职管理，包括：

a) 对其电脑等设备进行清查，对涉密载体及复制品、相关物品进行盘点；

b) 确认是否已签署保密协议，如未签署需补签；

c) 评估是否需要履行竞业限制协议或与其重新签署竞业限制协议；

d) 与其签署保密承诺书，要求其声明不再拥有任何与商业秘密相关的载体；

e) 离职面谈，告知其负有的保密义务，以及其他约定或法定的注意事项；

f) 对其离职后去向进行定时追踪，及时发现商业秘密泄密或不正当使用的线索。

企业应保留涉密人员离职管理的成文信息。

9.3 涉密载体管理

9.3.1 总则

企业对涉密载体进行管理时应：

a) 明确涉密载体及其功能作用，制定涉密载体管理制度；

b) 确定涉密载体的保护要求；

c) 建立涉密载体台账；

d) 由专人负责管理；

e) 实施涉密载体的制作、收发、传递、使用、复制、保存、维修、销毁的全生命周期管理。

企业应保留可证明涉密载体管理的成文信息。

9.3.2 制作

企业在制作涉密载体时，应确保：

a) 明确保护措施、应实施的控制要求和管理权限；

b) 根据商业秘密的级别对不同涉密载体明确使用或发放范围和制作数量；

c) 在涉密载体的相关位置标注商业秘密的标志或信息，必要时可使用隐藏式记号。

企业应保留涉密载体制作的成文信息。

9.3.3 收发、传递

涉密载体的收发应履行清点、编号、登记、签收手续。

企业应保留涉密载体收发、传递的成文信息。

9.3.4 使用

使用涉密载体时应办理手续。

携带涉密载体外出或外发涉密载体时，应履行审批手续；并对涉密载体的流转过程进行记录，确保外发的涉密载体使用完毕后及时回收。

企业应保留涉密载体使用的成文信息。

9.3.5 复制

涉密载体的复制应符合下列要求：

a） 涉密载体复制时，应履行审批、登记手续；

b） 复制涉密载体不得改变商业秘密的密级、保密期限和知悉范围；

c） 涉密载体复制件应加盖复制戳记，并视同原件管理。

企业应保留涉密载体复制的成文信息。

9.3.6 保存、维修及销毁

涉密载体的保存、维修及销毁应符合下列要求：

a） 企业应选择安全保密的特定场所或位置保存涉密载体，并根据涉密载体的不同由专人保管；

b） 企业应定期清查、核对涉密载体；

c） 涉密载体需外部人员现场维修的，应指定专人全程现场监督；

d） 涉密载体的销毁应进行审核批准，并履行清点、登记手续；

e） 应确保销毁的秘密信息无法还原。

企业应保留涉密载体保存、维修及销毁的成文信息。

9.4 涉密设备管理

9.4.1 显性涉密设备

企业应对生成、存储、处理商业秘密的显性设备进行保密管理，包括：

a） 设定涉密设备安全管理政策，以保证商业秘密不受损害或侵害；

b） 设定信息加密系统以确保商业秘密均经过加密处理，并限制信息的存储和复制等操作；

c） 设定员工权限管理系统，并定期更换密码，以保证仅有权限的员工才能接触到相应的商业秘密；

d） 提供专门的工作用设备和沟通交流方式；

e） 对员工访问商业秘密进行追踪、检测和备案；

f） 在软件开发过程中应注意信息安全；

g） 注意网络和通信安全，防止内部、外部入侵；

h） 将监管系统告知员工，保证合法性的同时及时发现员工违反安全措施并留存证据；

i） 实施涉密设备的使用、维修、报废的全生命周期管理。

企业应保留涉密设备管理的成文信息。

9.4.2 隐性涉密设备

企业应对通过观察或者测试、分析手段能够获得商业秘密的设备或产品进行保密管理，包括：

a） 在采购过程中通过签订保密协议，采购混淆成分，隐藏采购人名称、地址和项目名称、用途等方式来降低泄密风险；

b） 在运输过程中通过遮挡、与承运方签订保密协议等方式降低泄密风险；

c） 在调试试验或使用过程中通过遮挡、限制区域和进入人员等方式降低泄密风险；

d） 报废前进行脱密处理。

9.5 涉密区域管理

企业应对涉密区域进行管理，包括：

a) 划分并确定涉密区域及其分级，不同级别涉密区域放置不同警示标志，涉密区域与普通区域以明显警示标志隔离；

b) 通过警报、门禁等安防措施加强涉密区域的出入管理：对于内部人员，应当根据分类分级进行不同的进出管理；对于外部人员，应进行前置审批、登记并制作识别证件，明确可以获取的信息范围、活动范围和路线，并由工作人员陪同；访客离开时若有随身携带的物品，应对其进行检查；

c) 可设置监测系统，对涉密区域的入口和主要通道等实行管控。

企业应保留涉密区域管理的成文信息。

9.6 对外合作的商业秘密管理

9.6.1 信息发布

企业应对信息的对外发布进行管理，包括：

a) 建立信息对外发布的保密审查责任制，明确信息对外发布的保密审查程序和主管领导、机构和工作人员；

b) 信息对外发布前应当确认信息是否经过保密审查，并做好商业秘密对外发布的保密审查相关记录的留存和备案工作；

c) 企业应对信息对外发布进行经常性保密检查，发现问题立即采取补救措施；

d) 应确保对外发布的商业秘密进行有效追踪。

企业应保留信息对外发布的成文信息。

9.6.2 商务活动

采购、销售、委托开发、委托生产、参展等商务活动中的商业秘密管理包括：

a) 在开始商务谈判前或提供商业秘密前，应与对方签署保密协议；

b) 在参展过程中通过遮挡、与展览方签订保密协议等方式降低泄密风险；

c) 注意证据的留存；

d) 对协议履行过程中商业秘密的使用情况及泄露情况进行监督管理。

企业应保留商务活动中商业秘密管理的成文信息。

9.6.3 技术合作

技术合作中的商业秘密管理包括：

a) 调查合作方的商业秘密管理能力，优先选择通过商业秘密管理体系认证的合作方；

b) 约定背景商业秘密和共同开发、改进或二次开发中涉及商业秘密的内容和归属，必要时可对保密内容签署单独的保密协议；

c) 约定对共有商业秘密的管理，许可、转让或与第三方合作，争议处理等；

d) 商业秘密所有人应承诺其商业秘密不侵犯第三方任何权利。

企业应保留技术合作中商业秘密管理的成文信息。

9.6.4 国际交往

企业在准备发展国际业务时，应调查对方国家有关商业秘密的法律法规及执行情况，必要时可咨询

当地的专业人员。

9.6.5 企业并购重组

在并购或重组过程中，企业应：

a) 开展商业秘密尽职调查，对其法律、经济价值及风险进行评估；

b) 在接洽前应签署保密协议，协议应涉及商业秘密内容与范围、权利归属、利益分配方案、协议期限外的保密义务、争议解决途径、违约金及损害赔偿等；

c) 在并购或重组过程中做好文件交接记录和会议纪要，并形成保密文件清单；

d) 关注并购重组对象的涉密人员去向。

企业应保留保密协议、交接记录、会议纪要、保密文件清单等的成文信息。

9.6.6 许可、转让

许可或转让过程中，企业应：

a) 对商业秘密进行资产评估；

b) 在接洽前应签署保密协议，协议应涉及商业秘密内容与范围、权利归属、协议期限外的保密义务、争议解决途径、违约金及损害赔偿等；

c) 在许可或转让过程中做好文件交接记录和会议纪要，并形成保密文件清单。

企业应保留保密协议、交接记录、会议纪要、保密文件清单等的成文信息。

10 商业秘密的争议处理

10.1 侵权风险防范及应急处置

10.1.1 侵权风险防范

企业应采取措施，及时发现并防范商业秘密被侵权的情况，减少被诉风险：

a) 通过外部网络监控是否存在涉嫌商业秘密泄露的行为；

b) 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和维权部门；

c) 培训和引导员工在发现涉嫌被侵犯商业秘密后及时提供线索给维权部门；

d) 建立内外部举报机制，对于举报相关侵犯商业秘密的行为给予奖励；

e) 对于外部商业敏感信息，应及时核实其合法来源；对于合法获取的外部商业秘密，及时检查各使用环节是否符合相关法律及合同要求。

10.1.2 应急处置

企业应制定商业秘密泄密或被侵权的应急处置预案，建立紧急应对流程。泄密或被侵权事件一旦发生，应迅速进行处置，将危害控制在最小范围内。涉及国家秘密的，应立即向当地公安机关、国家安全机关和保密行政管理部门报告，并采取补救措施。

企业应保持应急处置的成文信息。

10.2 维权

10.2.1 侵权评估

发现商业秘密涉嫌被侵权时，企业应分析商业秘密是否受到侵犯以及评估受侵害的程度。包括：

a) 确定被侵犯的商业秘密是技术秘密还是经营秘密；
b) 确定被侵犯的商业秘密的范围及具体内容；
c) 商业秘密被侵犯的方式，如是否被披露给第三方、被公开、被使用等；
d) 侵权嫌疑人的情况；
e) 商业秘密被侵犯对企业造成的损害和影响；
f) 其他用来判定是否构成商业秘密侵权的因素。

10.2.2 维权途径

企业应根据侵权判定的结果确定采取的维权途径，维权途径可包括：
a) 与侵权人协商解决；
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) 根据仲裁条款或仲裁协议提请仲裁机构仲裁；
f) 向人民法院提起民事诉讼；
g) 向公安机关控告；
h) 申请人民检察院对商业秘密诉讼活动进行监督等。

10.2.3 确定维权方案

企业应根据确定的维权途径形成维权方案，包括：
a) 成立专项工作组，确定工作组人员、工作机制和工作分工；
b) 维权目标；
c) 维权措施，包括取证措施、维权策略等；
d) 时间计划及重要节点；
e) 是否聘请律师团队；
f) 资金预算等。

维权方案可根据案件进展进行动态调整。

10.2.4 侵权证据收集

企业可根据维权方案，确定证据收集的内容、范围和方式：
a) 企业是商业秘密的权利人的证据，包括体现商业秘密的载体、电子数据、存证证明等，必要时可进行数据提取；
b) 商业秘密具有经济价值的证据，包括具有现实或潜在的经济价值，必要时可委托评估机构进行价值评估；
c) 商业秘密不为公众所知悉的证据，必要时可委托鉴定机构出具非公知性鉴定报告；
d) 企业采取的保密措施，包括保密制度、保密协议以及其他保密措施；
e) 泄密人员相关信息，包括签订劳动合同、保密协议、具体工作职责、工作总结、能够接触商业秘密信息的证据等；
f) 研发证明或合法来源证明等；
g) 商业秘密被侵犯的证据，包括被披露或被使用的证据、泄密途径等，必要时可委托鉴定机构出具同一性鉴定报告；

h） 商业秘密被侵犯的损害事实，包括侵权行为具体表现，被侵权所受的损失或侵权行为所获得收益等，必要时可委托评估机构或审计机构进行损失鉴定等。

企业应保留侵权证据的成文信息。

10.3 应诉

10.3.1 应诉方案

根据被诉事件对企业造成的影响，以及侵权事实的判定结果，确定应诉方案。

10.3.2 应诉证据收集

在侵犯商业秘密诉讼中，被控侵权企业可从以下几个方面收集抗辩证据：

a） 证明权利人的信息并不构成商业秘密；

注：不构成商业秘密的情形包括：该信息在所属领域属于一般常识或者行业惯例的；该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；该信息已经在公开出版物或者其他媒体上公开披露的；该信息已通过公开的报告会、展览等方式公开的；所属领域的相关人员从其他公开渠道可以获得该信息的。

b） 相关信息为自主研发的证据材料；

c） 鉴定报告存在足以影响鉴定结论公正性的程序或实质问题，必要时可申请重新鉴定；

d） 企业自身不存在侵权主观故意的证据材料，如相关人员的保密承诺等。

企业应保留应诉的成文信息。

10.4 商业秘密司法鉴定

在商业秘密争议处理过程中，需要进行司法鉴定的，可委托有资质的鉴定机构对所涉信息是否为公众所知悉，被告获得、披露、使用的信息与原告持有的信息是否相同或者实质相同等进行司法鉴定。

企业应保留司法鉴定的成文信息。

10.5 制度完善

企业应根据商业秘密争议过程中发现的管理问题，及时对商业秘密管理制度进行补充完善。

11 监督检查、评审及改进

11.1 总则

企业应确定监督检查的准则和方法，定期检查商业秘密管理体系的运行情况并评审其绩效和有效性。

11.2 监督检查

企业应建立监督检查的准则并执行，以评价商业秘密管理绩效及商业秘密管理政策的有效性，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。

11.3 评审

11.3.1 安全度

企业应收集并测量商业秘密的安全度，测量指标可包括：

a） 涉密人员、载体、设备、区域、合同管理的覆盖率等；

b） 失泄密事件等级、数量占企业商业秘密总数的比例等。

企业应保留安全度测量的成文信息。

11.3.2 评价

企业应根据监督检查的结果评价商业秘密管理体系的绩效和有效性，包括：

a） 策划是否得到有效实施；

b） 应对风险和机遇所采取措施的有效性；

c） 商业秘密的安全度；

d） 商业秘密管理体系改进的需求。

企业应保留监督检查及评审的成文信息。

11.4 改进

当发生不符合时，企业应对不符合进行评审，确定不符合的原因以及类似的不符合是否存在或可能发生，并采取措施控制和纠正不符合。

企业应持续改进商业秘密管理体系的适宜性、充分性和有效性，不断提升商业秘密管理的安全度。

参 考 文 献

[1] GB/T 1.1 标准化工作导则 第1部分:标准化文件的结构和起草规则

[2] GB/T 19000 质量管理体系 基础和术语

[3] GB/T 20000.1 标准化工作指南 第1部分:标准化和相关活动的通用术语

[4] GB/T 20004.1 团体标准化 第1部分:良好行为指南

[5] GB/T 22080 信息技术 安全技术 信息安全管理体系 要求

[6] GB/T 29490 企业知识产权管理规范

[7] GB/T 33250 科研组织知识产权管理规范

[8] GB/T 33251 高等学校知识产权管理规范

[9] GB/T 34061.1 知识管理体系 第1部分:指南

[10] T/CAS 1.1 团体标准的结构和编写指南

[11] 中华人民共和国反不当竞争法

[12] 黄武双.商业秘密保护的合理边界研究[M].北京:法律出版社,2018.

[13] 王冰,王博. 完美的商业秘密管理:商业秘密保护与纠纷预防[M]. 武汉:武汉大学出版社,2008.

[14] 马克·R.哈里根,理查德·F.韦加德. 商业秘密资产管理(2016):信息资产管理指南[M]. 北京:知识产权出版社,2017.

[15] 周立权.商业秘密保护指南[M]. 北京:中国社会出版社,2019.

[16] 王润华.第四知识产权:美国商业秘密保护[M].北京:知识产权出版社,2021.

[17] 北京市知识产权维权援助中心.企业商业秘密管理工作指引[M]. 北京:知识产权出版社,2020.

华信金泰检验认证有限公司

Huaxin Jintai Inspection and Certification Co., Ltd.

保密管理体系要求

文件编号：CTS HXJT/YQMS-13-2026

文件版次：A/0

编　　制：文件编制小组

审　　核：

批　　准：

受控状态：受控

发布日期：2026 年 03 月 18 日　　实施日期：2026 年 03 月 18 日

文件修改记录

修订说明	修订页数	修订日期	批准

目录

地址： 河北省石家庄市长安区广安街 91 号世纪方舟 B-26-2203,2206

电话：0311-68008520 邮箱：hxjttc@hxjttc.com