ICS 03.100.01
CCS A 01

DB3301

浙 江 省 杭 州 市 地 方 标 准

DB3301/T 0496—2025

商业秘密保护能力指标体系

2025-06-30 发布　　2025-07-30 实施

杭州市市场监督管理局　　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。

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。

本文件由杭州市公安局提出、归口并组织实施。

本文件起草单位：杭州市公安局、公安部第三研究所、浙江省杭州市中级人民法院、浙江省杭州市人民检察院、杭州市司法局、杭州市市场监督管理局、浙江工商大学、杭州海康威视数字技术股份有限公司、新华三技术有限公司。

本文件主要起草人：郑嵘、何盛、张汀、陶春和、潘才敏、吕后旺、王毅、谢轶、王晴、缪志鹏、方伟、牛强、刘文琦、程晓萍、沈协栋。

商业秘密保护能力指标体系

1 范围

本文件规定了商业秘密保护能力指标体系的总则、指标体系、结果运用与持续改进。

本文件适用于企业衡量商业秘密保护能力。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DB33/T 2273 商业秘密保护管理与服务规范

3 术语和定义

DB33/T 2273界定的术语和定义适用于本文件。

4 总则

4.1 科学性

指标体系构建应科学合理，能全面、准确、客观体现商业秘密实际的保护能力情况。

4.2 适用性

指标的设定和选取应适当可行，能结合实际进行信息与数据采集，并开展定性定量分析。

4.3 可拓展性

指标体系可延伸和扩展，在指标体系运用过程中，不断总结指标体系的优缺点，阶段性地对指标体系进行调优、扩展，保持指标体系的先进性。

5 指标体系

5.1 指标体系概述

5.1.1 商业秘密保护范围主要为技术信息和经营信息，其表现形式按附录 A 执行。

5.1.2 应围绕提升企业商业秘密的保护能力，结合组织机构、制度建设、涉密信息、涉密人员、涉密区域、涉密载体、数字化能力、检查、改进等方面进行指标体系构建。

5.1.3 指标体系分为二层结构，其中一级指标 9 项，二级指标 37 项。

5.2 指标体系构成

商业秘密保护能力指标体系构成见表1。

表1　商业秘密保护能力指标体系构成表

序号	一级指标	二级指标	释义	必选项
1	组织机构	岗位职责	成立商业秘密保护机构，并明确岗位职责	√
2		保密意识	权利人或管理层具备商业秘密保护意识	√
3		保密能力	保密人员熟悉商业秘密管理制度，具备相关的保密设施使用能力	—
4		培训机制	制定培训工作机制，定期开展商业秘密保护专题培训	√
5	制度建设	制度实施	制定相关商业秘密管理制度并组织实施	√
6	涉密信息	信息识别	对涉密技术信息和涉密经营信息进行有效识别，识别商业秘密信息的具体内容及其范围	√
7		信息定级	根据商业秘密重要性，确定保护等级（核心秘密、重要秘密和一般秘密），在涉密信息上标注商业秘密保护等级，并定期复评、动态调整	—
8		技术查新	根据技术秘密特征点及更新程度，定期进行查新检索，明确保护技术重点	—
9		信息附增	在客户名录上附增交易习惯、交易需求等深度信息，综合保护经营信息	—
10	涉密人员	人员识别	应当根据员工的岗位职责、工作内容，以及接触涉密信息的可能性确定涉密人员	—
11		协议签订	与涉密岗位员工签订保密合同/协议，涉密重点岗位员工（如职业经理人、技术、采购、销售等）可签订竞业限制协议	√
12		协议要求	保密合同/协议明确商业秘密范围和商业秘密保护的义务	√
13		分级管理	根据涉密岗位、涉密人员接触涉密信息的重要性，实行分级管理	—
14		人员异动	涉密人员调岗或离职时，开展必要的行为审计，审查启动竞业协议必要性，跟踪离职去向等	—
15	涉密区域	监控报警装置	涉密区域的监控、报警等设备运行良好，监控日志及监控储存信息与涉密人员的活动一致	√
16		物理隔离	涉密区域设置有效的物理隔离保密措施，包括但不限于门禁系统、独立操作间、窗户防窥膜等，绝密区域应当设置双人验证或二级授权门禁	—
17		登记提醒	涉密重点区域实行进出登记和保密告知提醒	—
18		张贴标识	在涉密区域醒目位置张贴区域警示标识和行为禁止标识	√
19		行为禁止	企业员工知悉涉密区域属性和行为禁止要求	—
20		区域审批	非相关人员进入涉密区域，设置权限并履行审批手续，并对进入后的活动区域加以限制	—
21	涉密载体	对象选择	根据工作实际需求对涉密载体发放对象进行明确	—
22		警示标志	涉密载体标注涉密警示标志并划分涉密等级	—
23		知悉要求	接触涉密载体的企业员工知悉载体涉密属性及保密要求	—

表1　商业秘密保护能力指标体系构成表（续）

序号	一级指标	二级指标	释义	必选项
24	涉密载体	使用权限	设置涉密载体的使用权限，明确使用人、管理人、责任人，履行审批手续，对长期使用涉密载体，不定期开展监督检查，对确因工作需要而临时性使用涉密载体的，严格审查必要性及事由	√
25		物品管理	对半成品、加工件、物料等涉密物品进行妥善管理	√
26		使用记录归档	能全程记录涉密载体的使用日志，妥善做好归档保存	√
27		回收检查	涉密员工离职时对企业配发的涉密载体予以回收并检查	√
28		销毁清除	对涉密载体、物品进行定期销毁清除，相关记录留存备档	√
29	数字化能力	数字防护技术部署与应用	在核心信息系统、网络、终端设备上部署和应用专门用于商业秘密保护的数字化技术，包含但不限于强认证技术、加密技术、明暗水印技术、网络边界监控和过滤技术等	—
30		自动化识别与分类	利用内容识别引擎、元数据分析等技术自动或者半自动地识别、标记、分类商业秘密信息	—
31		细化访问控制与权限管理	利用身份与访问管理体系、权限管理系统、零信任架构等技术，对商业秘密数据进行最小权限、基于角色/属性/情境的动态访问控制	—
32		异常行为检测	利用大数据分析及人工智能技术对日志、用户行为、安全事件持续监控分析，有效检测并告警异常行为或者高风险事件	—
33		灾难备份	建立有效的灾难恢复计划，对核心商业秘密数据进行安全可靠备份，确保在遭受勒索软件攻击、系统故障、自然灾害等情况下，商业秘密数据能够被快速恢复，保障业务持续性	—
34	检查	行为监督、活动核查	对员工涉密行为进行监督、对涉密活动的记录进行核查	—
35		设备检查、维护	对涉密场地的设施设备进行检查和维护	—
36		开展内部审计	定期开展商业秘密保护能力的内部审计活动	—
37	改进	改进措施	针对检查或演习发现的问题制定改进措施，并予以实施	—

6　结果运用与持续改进

6.1　结果运用

6.1.1　依据行业特性，企业应定期根据指标体系及相关资料，采用专家打分法、模糊综合评判法、自陈报告法等方法，确定二级指标与指标权重进行能力自查。商业秘密保护准备资料汇总表见附录 B。

6.1.2　应重点针对管理流程薄弱环节、风险漏洞等方面，提出防范工作建议。

6.2　持续改进

6.2.1　企业可根据结果运用情况开展自身的持续改进。

6.2.2　在指标体系运用过程中发现问题的，应针对问题项进行原因分析，并制定切实可行的改进方案。

附 录 A
（规范性）
商业秘密保护范围

A.1 技术信息

商业秘密的技术信息保护范围应符合表A.1的规定。

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、样机、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、实物原型、半成品样件、物料等

A.2 经营信息

商业秘密的经营信息保护范围应符合表A.2的规定。

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
采购经营信息	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、各类账册、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）
商业秘密保护资料汇总表

表B.1给出了商业秘密保护资料汇总表。

表B.1 商业秘密保护资料汇总表

序号	材料名称及内容	说明内容
1	具备法人或非法人经济组织的营业执照和工商注册登记文件、身份证明等	说明权利人主体身份和资格
2	提供商业秘密信息内容说明。对于技术信息，应包含该信息的组成要素、形成的技术背景、涉及的技术领域、创新部分和“秘密点”的技术特征。（可委托具有专业资质的服务机构做查新报告或非公知性鉴定报告进行说明；对于经营信息，需提供经营信息原创性说明材料）	说明商业秘密存在且成立，具备不为公众所知悉性
3	提供商业秘密价值性说明（企业为获得该信息，付出一定经济成本的证明）	说明商业秘密存在且成立，具备价值性
4	提供商业秘密保密措施说明（企业为保护商业秘密所采取的保密措施，包括制度设定、措施执行、保密约定、保密费用支付等）	说明商业秘密存在且成立，具备保密性
5	具备企业内部商业秘密管理规章制度、工作机制及操作规范等	说明企业建立内部保密工作机制
6	具备涉密员工保密培训记录、劳动合同、保密协议、竞业限制等	说明企业针对涉密员工开展保密工作
7	具备涉密区域警示标志、门禁系统、电子监控等	说明企业针对涉密场所开展保密工作
8	提供涉密载体/物品的保管人、使用人、责任人说明，使用、维修、销毁、清除审批手续等	说明企业针对涉密载体开展保密工作
9	提供涉密信息等级划分情况，且执行信息安全等级保护工作举措	说明企业针对涉密信息开展保密工作
10	提供针对计算机内部网络、企业邮箱、涉密邮件等采取的科技化保护措施说明	说明企业针对涉密网络开展保密工作