ICS 03.100.01
CCS A 01

DB32

江　苏　省　地　方　标　准

DB 32/T XXXX—2026

企业商业秘密风险防控规范

Specification for risk prevention and control of enterprise trade secrets

（报批稿）

2026 - XX - XX 发布　　2026 - XX - XX 实施

江苏省市场监督管理局　　发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　总体要求 2
5　组织与职责 2
6　定密管理 3
7　涉密人员风险防控 4
8　涉密载体风险防控 5
9　涉密区域风险防控 5
10　涉密信息化风险防控 6
11　外部合作与信息披露风险防控 7
12　应急处置 8
参考文献 9

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。

本文件由江苏省市场监督管理局提出、归口并组织实施。

本文件起草单位：南京大学、江苏省市场监督管理局、江苏省质量和标准化研究院、南京市市场监督管理局、无锡市市场监督管理局、苏州市吴江区市场监督管理局、无锡市半导体行业协会、苏州市吴江区智能制造协会、贝卡尔特（中国）技术研发有限公司、亨通集团。

本文件主要起草人：徐棣枫、陈琪宏、朱益俊、刘谦、杨玉龙、庞博、郭利华、韩玉坤、黄安君、马振华、王剑伟、徐勤锋。

企业商业秘密风险防控规范

1 范围

本文件规定了企业商业秘密风险防控的总体要求、组织与职责、定密管理、涉密人员风险防控、涉密载体风险防控、涉密区域风险防控、涉密信息化风险防控以及外部合作与信息披露风险防控、应急处置的要求。

本文件适用于企业开展商业秘密风险防控工作。

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。

GB/T 22080 网络安全技术 信息安全管理体系 要求

GB/T 22081 网络安全技术 信息安全控制

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31722 网络安全技术 信息安全风险管理指导

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35274 信息安全技术 大数据服务安全能力要求

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 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。

3.2

涉密人员 secret-related personnel

根据工作职责或者有关协议有权接触、使用、掌握企业商业秘密信息的企业员工或其他人员。

3.3

涉密载体 secret-related carrier

以文字、数据、符号、图形、图像、视频和音频等方式记载企业商业秘密信息的各类介质，包括纸质文档、电子文件、存储介质、设备及其他形式的载体。

3.4

涉密区域 secret-related area

企业开展日常经营、制作、生产、传递、使用、存放、保管商业秘密涉密载体等的区域。

3.5

保密协议 non-disclosure agreement

企业与员工、合作方等主体之间就商业秘密保护的权利义务所订立的书面协议。

4 总体要求

4.1 主体责任

企业是商业秘密风险防控的责任主体，宜建立商业秘密风险防控制度并纳入日常管理，自主确定组织领导机制、防控范围、期限、区域等。

4.2 预防优先

应以风险预防为核心，加强风险识别与预警，降低泄密风险。

4.3 定期评估

企业应依据 GB/T 31722 定期开展商业秘密保护风险评估，识别内部管理和外部环境中的泄密风险点，应明确风险处置的责任部门、整改措施和完成时限。

5 组织与职责

5.1 通则

企业宜结合组织架构、经营规模和业务特点，建立商业秘密风险防控决策层、风险防控管理层和风险防控操作层三级组织体系。

5.2 风险防控决策层

风险防控决策层由企业主要负责人（法定代表人或实际负责人）担任负责人，分管保密工作的负责人任负责人，相关部门负责人为成员。风险防控决策层确定商业秘密风险防控的愿景、使命、战略、方针和目标，开展全局性、方向性、决策性工作，主要职责包括：

a） 审定商业秘密风险防控基本管理制度、重大防控措施和专项工作方案；
b） 确定商业秘密风险防控工作的目标、任务和年度重点工作安排；
c） 组织协调商业秘密风险防控资源投入，保障人员、经费、技术和设施设备的配置；
d） 监督检查商业秘密风险防控制度执行情况，听取风险防控管理层工作汇报；
e） 决定商业秘密侵权应急处置中的重大事项，审定重大泄密事件的处理意见。

5.3 风险防控管理层

风险防控管理层执行风险防控决策层的决策，对日常工作进行计划、组织、控制、协调，主要职责包括：

a） 起草、修订商业秘密风险防控制度并组织实施；
b） 对识别的商业秘密信息进行审核批准；
c） 调查处理泄密事件，协助维权工作；
d） 管理保密档案和相关资料。

5.4 风险防控操作层

风险防控操作层宜在风险防控决策层的领导下、风险防控管理层的组织管理下，负责部门具体执行和操作工作，相应人员宜具备法学、知识产权管理或相关专业背景及实务经验，熟悉商业秘密保护法律法规。其主要职责包括：

a） 负责部门商业秘密的识别、确定、管理和监督检查；

b） 制定部门商业秘密识别具体方案，定期开展自查，发现问题及时整改；
c） 严格遵守商业秘密风险防控制度和操作规程，妥善保管涉密载体和涉密信息，落实各项保密措施，发现泄密隐患或泄密事件及时报告。

6 定密管理

6.1 定密管理流程

按下列程序实施：
a） 商业秘密识别；
b） 商业秘密审核；
c） 密级划分；
d） 保密期限确定；
e） 标识管理；
f） 商业秘密清单确定；
g） 动态调整。

6.2 商业秘密识别

各部门对经营活动中产生的各类商业信息进行识别，识别方法包括但不限于科技查新、经验分析、专利与非专利技术比对、公开文献检索、行业惯例分析、专家评估等。

6.3 商业秘密审核

商业秘密的确定应由形成该信息的业务部门提出申请，经风险防控管理层审核批准。

6.4 密级划分

企业宜根据商业秘密信息的重要程度、泄露后可能造成的经济损失程度，将商业秘密划分为以下三个等级。
a） 一级：泄露将导致企业遭受特别严重经济损失的核心商业秘密，如核心产品配方、关键源代码、重大研发战略等。
b） 二级：泄露将导致企业遭受严重经济损失的重要商业秘密，如重要工艺流程、主要客户信息、关键经营数据等。
c） 三级：泄露将导致企业一定经济损失的一般商业秘密。

6.5 保密期限确定

企业宜根据商业秘密的密级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，确定保密期限。

6.6 标识管理

企业宜在涉密载体上标注密级、保密期限及保密警示信息。标识应清晰、醒目、不易去除。电子文件宜采用数字水印、元数据标注等方式标注密级。

6.7 商业秘密清单确定

企业宜建立商业秘密清单，对商业秘密信息登记，并根据信息变化及时更新清单。清单内容应包括：商业秘密名称、密级、产生部门、责任人、保密期限、知悉范围、载体形式、存储位置等。

6.8 动态调整

商业秘密密级、期限应实行动态调整，履行审批登记程序，并及时更新商业秘密清单和相关标识。出现下列情形之一的，应及时解密：

a) 保密期限届满没有延续的或商业秘密信息已公开的；
b) 信息已丧失商业价值；
c) 被新技术替代已无保护必要的。

7 涉密人员风险防控

7.1 涉密人员分类

企业宜根据岗位性质和接触商业秘密的程度，将涉密人员分为以下类别。

a) 核心涉密人员：接触一级商业秘密的人员。
b) 重要涉密人员：接触二级商业秘密的人员。
c) 一般涉密人员：接触三级商业秘密的人员。

7.2 入职管理

7.2.1 核心涉密人员或重要涉密人员入职前，应调查其工作经历、竞业限制及保密义务情况，包括但不限于过往任职单位、担任职务、是否签订保密协议或竞业限制协议。背景调查中个人信息收集、处理应符合 GB/T 35273 的规定。

7.2.2 涉密人员入职时应签订保密协议或在劳动合同中约定保密条款，明确保密范围、期限、义务及违约责任。宜与核心、重要涉密人员签订竞业限制协议。

7.2.3 应划定新员工商业秘密知悉的基础范围，不宜安排试用期员工参加企业重要涉密会议或核心研发任务。

7.3 在职管理

7.3.1 企业宜制定涉密岗位及涉密人员清单，并根据人员入职、离职、岗位调整等情况及时更新清单。

7.3.2 企业宜定期开展保密教育培训。培训内容包括但不限于：

a) 商业秘密风险防控法律法规及企业保密制度；
b) 泄密风险识别与防控措施；
c) 泄密典型案例警示教育；
d) 保密要求。

7.3.3 人员调入涉密岗位前应进行保密教育和业务培训，办理涉密资产交接。

7.4 离职管理

企业应制定明确的离职涉密管理流程，具体措施包括但不限于：

a) 在员工离职前确定其是否涉密及涉密范围，评估泄密风险，决定履行或解除竞业限制协议；
b) 督促离职涉密人员移交全部涉密资料、存储介质和工作成果，如在研项目技术方案、实验记录及源代码等，办理涉密资产交接。移交过程由专人监督，保障移交完整、无遗漏；
c) 及时注销离职人员的系统账号、门禁权限，回收门禁卡、密钥等；

d) 对核心、重要涉密人员进行离职面谈，重申保密义务和竞业限制要求，告知泄密法律责任；面谈记录应经双方签字确认并归档；不应限制员工运用个人积累的通用知识、技能与经验；
e) 对负有保密义务的离职人员，掌握其任职信息，监督保密义务执行情况；对签订竞业限制协议的人员，按约定支付补偿金并进行跟踪管理；
f) 建立离职风险预警机制，对核心涉密人员的离职动向予以跟踪关注。对离职员工入职竞争对手的情况，评估泄密风险，必要时采取应急处置措施。

示例：核心研发人员离职应移交在研项目技术方案、实验记录及源代码，清点个人备份介质，注销代码仓库、研发数据平台访问权限。

7.5 其他人员

企业宜将与本企业无劳动合同关系但可能接触知悉商业秘密的人员，纳入涉密人员管理，包括但不限于：

a) 劳务派遣人员、外包服务机构驻场人员；
b) 实习见习人员、退休返聘及兼职人员；
c) 外部顾问专家、合作方派驻人员。

8 涉密载体风险防控

8.1 纸质文档管理

8.1.1 涉密纸质文档应分类管理，标注密级和保密期限，存放于专用保密柜并由专人管理。
8.1.2 制作、复制、借阅、传递、保存、销毁涉密纸质文档应履行审批登记程序。
8.1.3 传递涉密纸质文档应使用专用封装，由专人送达。

8.2 电子文件管理

8.2.1 涉密电子文件的制作、编辑、存储、传输应履行审批登记程序，采取加密措施，设置访问权限，留存操作日志。
8.2.2 涉密电子文件对外传输应在履行审批登记程序后，采用加密通道并由专人发送。

8.3 存储介质管理

8.3.1 存储商业秘密的载体，如U盘、硬盘、光盘、磁盘等介质应登记造册，实行标签化管理，标注密级和责任人。
8.3.2 存储介质的使用、维修、报废应履行审批登记程序。报废存储介质应进行物理销毁或数据彻底擦除。
8.3.3 不应使用个人存储介质存储、传输涉密信息。

8.4 设备、产品和信息系统管理

对直接含有商业秘密信息或通过观察、测试、分析能够获得商业秘密信息的设备、产品和信息系统，应详细记录其名称、型号、密级、保密期限、访问权限等信息，由专人管理，存放于专门存储区域，采取有效隔离和防控措施。

示例：研发载体包括样机、试制品、模具等，应统一编号、登记入台账，带离实验室应履行审批登记程序。

9 涉密区域风险防控

9.1 区域划分

企业宜根据岗位性质和涉及商业秘密的程度，将涉密区域分为以下类别。

a) 核心涉密区域：涉及一级商业秘密的区域。
b) 重要涉密区域：涉及二级商业秘密的区域。
c) 一般涉密区域：涉及三级商业秘密的区域。

9.2 区域管控

企业宜根据涉密区域等级实施差异化管控，管控措施的严格程度与区域等级相对应。

a) 物理隔离与防护：涉密区域宜与其他工作区域物理隔离，按区域等级配置门禁系统、视频监控、入侵报警等安全防护设施，核心涉密区域宜采取最高等级的物理隔离措施。
b) 标识管理：各级涉密区域入口处应设置清晰、醒目的警示标识和保密提示，并标注区域等级。
c) 人员管控：涉密区域人员流动应符合保密要求；进入核心、重要涉密区域应履行审批登记程序，核心涉密区域实行双人双锁管理；一般涉密区域的管控措施可适当简化。
d) 设施设备配置：核心、重要涉密区域应配备专用保密柜、碎纸机、电磁屏蔽设备等安全设施。
e) 电子设备管理：核心涉密区域应设置专门存放区域，未经批准不应携带具有录音、录像、拍照、存储功能的设备进入；重要涉密区域宜参照执行。
f) 文印设备管理：涉密区域的打印、复印、扫描设备应指定专人管理，操作记录留存备查；核心、重要涉密区域的文印输出应履行审批登记程序。
g) 外部人员管理：外部人员进入涉密区域应履行审批登记程序，登记身份信息和来访事由，宜签署保密提示文件，由企业专人全程陪同，不应允许其单独停留；外部人员不应进入与其业务无关的涉密区域。
h) 涉密会议与活动：在涉密区域内召开涉密会议、开展涉密活动应履行审批登记程序，明确参加人员范围；会前应进行保密检查，不应带入或使用具有录音、录像、拍照、存储功能的设备；涉密会议资料应编号发放，会后及时回收。

10 涉密信息化风险防控

10.1 数字化防控措施

10.1.1 企业宜运用互联网、大数据、云计算、人工智能、区块链等技术，推动商业秘密风险防控数字化转型，大数据处理活动应符合 GB/T 35274 的安全能力要求。

10.1.2 企业宜按照 GB/T 22081 选择适用的信息安全控制措施，对涉密信息实施自动识别分类、定密标识、权限管控、异常行为检测、备份恢复等技术防护措施，建立涉密信息清单，并对全流程执行审批与日志留存。

10.1.3 企业宜建立网络访问控制机制，对涉密系统实施身份认证、权限管理和操作审计。

10.2 电子存证

10.2.1 企业宜采用电子签名、可信时间戳等技术，对涉密信息的形成、使用、流转过程进行固定和存证，提升证据保全与取证能力。存证内容应包括涉密信息文件哈希值、存证时间、操作人员信息、操作类型等。

10.2.2 采用区块链存证的，应确保存证数据的完整性、不可篡改性和可追溯性，存证平台应具备相应资质。

10.2.3 企业宜通过公证机构办理涉密信息存证公证，提升证据效力。

10.3 网络和信息安全防护

10.3.1 企业宜按照 GB/T 22080 建立信息安全管理体系，部署防火墙、入侵检测、防病毒、数据防泄漏等安全设备，宜按照 GB/T 22239 落实网络安全等级保护基本要求。
10.3.2 企业宜定期开展网络安全风险评估和渗透测试，及时修复。
10.3.3 企业宜建立安全事件监测和响应机制，对异常访问、数据外发等行为实时告警和处置。

10.4 上云与软件运营服务（SaaS）管理

10.4.1 企业采用云服务、使用 SaaS 时，应评估服务商的数据安全能力，签订包含保密条款的服务协议。
10.4.2 数据迁移过程中应加密传输，迁移完成后验证数据完整性。
10.4.3 企业宜建立数据备份和灾难恢复机制，定期进行恢复演练。

10.5 人工智能应用管理

10.5.1 企业使用人工智能工具处理业务时，应评估数据输入的保密风险，不应将涉密信息输入公共人工智能平台。
10.5.2 企业宜建立人工智能工具使用审批制度，明确可使用的工具范围、数据处理边界和安全要求。

示例：研发实验数据实时写入研发数据平台，按项目逻辑隔离。使用人工智能辅助编程工具前应履行审批程序，仅可输入开源代码及脱密后的算法逻辑。

10.6 远程办公与数据出境

10.6.1 远程办公场景下，企业应要求员工使用经安全配置的设备和 VPN 通道访问涉密系统，不应在公共网络环境下处理涉密信息。
10.6.2 涉及跨境技术合作数据传输的，应遵守数据出境安全评估相关规定，履行必要的审批程序。
10.6.3 跨境数据传输宜采用加密通道，传输记录应留存备查。

11 外部合作与信息披露风险防控

11.1 外部合作管理

11.1.1 合作方准入管理

合作开始前，企业应对合作方进行保密资质审查，评估其保密能力和信誉状况。涉及商业秘密的合作项目，应签订保密协议，保密协议应明确：商业秘密范围、保密期限、保密义务、违约责任、争议解决方式等条款。

示例：联合研发项目立项时明确背景知识产权归属及改进成果权属，研发资料按密级分目录共享，按最小必要原则提供。

11.1.2 合作过程管理

合作过程中，企业应对保密协议履行情况进行监督。

11.1.3 合作后续管理

11.1.3.1 合作结束后，企业应依据保密协议处置商业秘密载体及信息，并出具确认书。
11.1.3.2 联合研发项目结束后，应按双方约定对商业秘密归属进行划分确认。

11.2 外部信息披露

11.2.1 向外部披露商业秘密应遵循最小必要原则，明确披露范围、保密义务、使用限制和返还销毁要求。

11.2.2 在信息发布、商业合作、技术合作、融资上市及并购重组等需要向外部提供商业秘密前，应签订保密协议，明确保密责任和义务。

11.2.3 信息披露应由业务部门申请，经风险防控管理层相关负责人审批。

11.3 境外保密协议与争议解决

企业应与境外合作方签订符合国际惯例的保密协议，明确适用法律和争议解决方式。

12 应急处置

12.1 应急事件处置

12.1.1 应急预案

企业宜制定商业秘密被侵犯后应急处置预案，明确应急响应流程、责任人和处置措施。

12.1.2 应急措施

发现商业秘密被侵犯后，应立即启动应急预案，采取以下措施：

a) 立即控制事态范围，防止损失扩大；

b) 启动内部调查，查明原因和责任人员；

c) 保存相关证据，记录事件发生的时间、地点、涉及人员和信息内容；

d) 评估损失和影响，确定权利救济策略与途径。

12.1.3 应急演练

企业宜定期开展应急演练，提升应急处置能力。

12.2 权利救济途径

12.2.1 民事救济

商业秘密权利人宜通过以下民事救济途径维护自身合法权益。

a) 民事诉讼：依照《中华人民共和国民法典》《中华人民共和国反不正当竞争法》等法律法规向人民法院提起民事诉讼。

b) 调解仲裁：可向人民调解组织、行业协会等申请调解；合同或保密协议中订立仲裁条款的，可依法申请仲裁；涉及竞业限制、保密义务等劳动争议的，依法申请劳动仲裁。

12.2.2 行政救济

依照《中华人民共和国反不正当竞争法》等法律法规规定向市场监督管理部门投诉举报。

12.2.3 刑事救济

对涉嫌侵犯商业秘密犯罪的，向公安机关报案。

参 考 文 献

[1] GB/T 24421　服务业组织标准化工作指南 第2部分：标准体系构建

[2] GB/T 29490—2023　企业知识产权合规管理体系要求

[3] 《中华人民共和国反不正当竞争法》

[4] 《中华人民共和国劳动合同法》

[5] 《中华人民共和国数据安全法》

[6] 《中华人民共和国个人信息保护法》

[7] 《中华人民共和国刑法》（侵犯商业秘密罪相关条款）

[8] 《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》（最高人民法院法释〔2020〕7号）

[9] 《商业秘密保护规定》（国家市场监督管理总局令第126号）

[10] 《江苏省市场主体商业秘密保护指引》（江苏省市场监督管理局）