

企业商业秘密保护通用规范

Specification of trade secret protection for enterprise

（征求意见稿）

2026 - XX - XX 发布

2026 - XX - XX 实施

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 总体原则 2

5 组织与职责 2

6 涉密人员管理 3

7 涉密载体与信息管理 4

8 商业秘密确定与分级 5

9 数据保护 6

10 物理安全与区域管理 7

11 合作方与外部管理 7

12 重点场景保护 8

13 风险识别与防控 9

14 应急处置与权利救济 9

15 检查与改进 10

参考文献 0

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。

企业商业秘密保护通用规范

1 范围

本文件规定了企业商业秘密保护的总体原则、组织与职责、确定与分级、涉密人员管理、涉密载体与信息安全管理、数据保护、物理安全与区域管理、合作方与外部管理、重点场景保护、风险识别与防控、应急处置与权利救济、检查与改进等要求。

本文件适用于江苏省行政区域内的各类企业开展商业秘密保护工作。其他类型的经营主体可参照执行。

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 22239 信息安全技术 网络安全等级保护基本要求
- 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

ISO/IEC 27005 信息安全、网络安全和隐私保护——信息安全风险管理指南（Information security, cybersecurity and privacy protection — Guidance on managing information security risks）

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。

注：商业秘密的构成要件、认定标准及具体释义，依照《中华人民共和国反不正当竞争法》及相关司法解释的规定执行。

3.2

权利人 right holder

依法对商业秘密享有所有权或者使用权的自然人、法人或者非法人组织。

3.3

涉密人员 personnel with access to trade secret

接触、知悉、掌握商业秘密的企业员工及其他相关人员。

3.4

涉密载体 secret carrier

以文字、数据、符号、图形、图像、视频和音频等方式记载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。

3.5

涉密区域 secret area

企业内部集中产生、流转、使用、存储、处理商业秘密信息的特定物理空间。

3.6

保密员 confidentiality officer

经企业指定，负责商业秘密保护日常管理工作的专职或兼职人员。

3.7

电子存证 electronic evidence preservation

运用电子签名、时间戳、区块链等技术手段，对商业秘密的形成、使用、流转等过程进行记录和固化的活动。

3.8

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 总体原则

4.1 企业主体

企业是商业秘密保护的责任主体，应建立商业秘密保护制度并纳入日常管理，自主确定组织领导机制、保护范围、期限、区域等。保护工作应覆盖企业各层级、各部门、各岗位。

4.2 预防优先

以防范为核心，坚持保护前移，注重风险识别与预警，降低泄密风险。

4.3 全生命周期管理

企业应将商业秘密保护融入研发、设计、采购、生产、销售、商务合作、人事、财务、法务等全业务过程，实现商业秘密的产生、流转、使用、存储、处理、销毁等全生命周期管理。

4.4 分级分类

根据商业秘密的重要程度、泄露影响程度，实行分级分类管理，合理配置保护资源，采取差异化的保护措施。

4.5 协同保护

建立企业、行业协会、第三方服务机构、行政机关、司法机关等多方协同的保护体系，形成全链条保护。

5 组织与职责

5.1 保密委员会

企业应设立保密委员会，由企业主要负责人（法定代表人或实际负责人）担任主任，分管保密工作的负责人担任副主任，相关部门负责人为成员。保密委员会的主要职责包括：

- a) 统筹领导企业商业秘密保护工作，审议批准商业秘密保护制度；
- b) 审批确定一级商业秘密及重大商业秘密事项；

- c) 组织协调商业秘密保护资源投入；
- d) 监督检查商业秘密保护制度执行情况；
- e) 决策商业秘密侵权应急处置中的重大事项。

5.2 商业秘密管理办公室

企业应指定专门机构（如知识产权管理部门、法务部门或行政管理部门）承担商业秘密管理办公室职能，配备专（兼）职保密员。商业秘密管理办公室的主要职责包括：

- a) 起草、修订商业秘密保护制度并组织实施；
- b) 组织商业秘密识别、定密、登记和清单管理；
- c) 开展保密宣传教育和培训；
- d) 监督检查各部门保密措施落实情况；
- e) 调查处理泄密事件，协助维权工作；
- f) 管理保密档案和相关资料。

5.3 保密员

保密员应具备法学、知识产权管理或相关专业背景，熟悉商业秘密保护法律法规。保密员的具体岗位职责包括：

- a) 执行商业秘密保护日常管理工作，协助开展商业秘密识别；
- b) 管理商业秘密清单，跟踪密级变更和解密情况；
- c) 审核涉密载体借阅、复制、流转等申请；
- d) 检查涉密区域的物理安全 and 信息系统安全；
- e) 协助开展保密培训和泄密警示教育；
- f) 参与泄密事件的初步调查和处理；
- g) 定期汇总分析保密工作情况，向管理办公室报告。

5.4 各部门职责

5.4.1 各部门负责人为本部门商业秘密保护的第一责任人，负责本部门商业秘密的识别、确定、管理和监督检查。

5.4.2 各部门应指定专（兼）职人员协助保密员开展本部门保密工作。

5.4.3 各部门应在职责范围内建立商业秘密识别机制，定期开展自查，发现问题及时整改。

6 涉密人员管理

6.1 涉密人员分类

企业应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。

6.2 入职管理

6.2.1 背景调查：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。调查应合法合规，尊

重个人隐私，背景调查中的个人信息收集、处理应符合 GB/T 35273 的规定。

6.2.2 保密承诺：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。建议与核心、重要涉密人员签订竞业禁止限制。

6.2.3 入职培训：涉密人员上岗前应接受商业秘密保护专项培训，培训内容包括保密制度、保密义务、泄密案例警示等，培训记录应存档备查。

6.3 在职管理

6.3.1 企业应制定涉密岗位及涉密人员清单，实行动态管理。

6.3.2 企业应定期开展保密教育和业务培训，强化保密意识。培训内容应包括：

- a) 商业秘密保护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（如员工跳槽引发侵权、研发人员泄露技术秘密等）；
- d) 新技术应用中的保密要求（如远程办公、AI 工具使用等）。

6.3.3 企业宜根据其企业规模、所属行业特点等灵活开展、参与各类培训，开展针对性内部培训。

6.3.4 涉密人员调岗前应进行保密提醒，明确新岗位的保密要求，做好涉密资产交接。

6.4 离职管理

6.4.1 离职审查：员工离职前应确定其是否涉密及涉密范围，评估离职风险，决定是否签订或启动竞业限制协议。

6.4.2 资料移交：离职涉密人员应移交全部涉密资料、存储介质和工作成果，做好涉密资产交接。移交应由专人监督，确保完整无遗漏。

6.4.3 权限清理：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。

6.4.4 离职面谈：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，但不得限制员工使用个人通用知识技能经验。面谈记录应签字确认并归档。

6.4.5 跟踪管理：对负有保密义务的离职人员，应掌握其任职信息，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。

7 涉密载体与信息管理

7.1 纸质文档管理

7.1.1 涉密纸质文档应分类管理，明确标识密级和保密期限。

7.1.2 涉密纸质文档的制作、复制、借阅、传递、保存、销毁应履行审批登记程序。

7.1.3 涉密纸质文档的传递应使用专用封装，由专人送达或通过机要渠道传送。

7.1.4 涉密纸质文档应存放于专用保密柜中，由专人管理。

7.2 电子文件管理

7.2.1 涉密电子文件的制作、编辑、存储、传输应经过审批，采取加密措施，设置访问权限，留存操作日志。

7.2.2 涉密电子文件的对外传输应采用加密通道，经过审批后由专人解密发送。

7.3 存储介质管理

7.3.1 存储商业秘密的 U 盘、移动硬盘、光盘等介质应登记造册，实行标签化管理，标注密级和责任

人。

7.3.2 商业秘密存储介质的使用、维修、报废应履行审批和登记手续。报废商业秘密存储介质应进行物理销毁或数据彻底擦除。

7.3.3 禁止使用个人存储介质存储、传输涉密信息。

7.4 设备、产品和信息系统管理

对于直接含有商业秘密信息，或通过观察、测试、分析手段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，放置于专门存储区域，采取有效隔离和保护措施。

8 商业秘密确定与分级

8.1 商业秘密识别

8.1.1 企业应组织各部门对经营活动中产生的各类商业信息进行识别，判断是否满足商业秘密的构成要件。《商业秘密保护规定》第五条规定所称的“商业秘密，是指不为公众所知悉、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。与技术有关的结构、原料、配方、材料、样品、样式、工艺、方法、数据、算法、计算机程序、代码等信息，属于第一款所称的技术信息。与经营活动有关的创意、管理、销售、财务、计划、样本、客户信息、数据等信息，属于第一款所称的经营信息。其中，客户信息包括客户的名称（姓名）、地址、联系方式以及交易习惯、意向、内容等信息。”

8.1.2 企业应区分个人通用知识、技能与企业专有知识的边界。员工通过个人学习、经验积累获得的通用行业知识、通用技能不属于企业商业秘密；但利用企业资源、在履行职务过程中形成的特有技术方案、客户信息、经营策略等应纳入商业秘密管理。

8.1.3 识别方法可包括但不限于：科技查新、经验判断、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。

8.1.4 职务性商业秘密与非职务性商业秘密权利归属如下。

- a) 职务性商业秘密是指员工执行本单位的任务或者主要利用本单位的物质技术条件所完成的商业秘密，其权利属于所在单位。
- b) 非职务性商业秘密是指员工在本职工作外，也未主要利用单位的物质技术条件完成的商业秘密，其权利属于完成该商业秘密的员工。

8.2 密级划分

企业应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大小和对企业竞争优势的影响程度，宜将商业秘密划分为以下三个等级，企业可根据实际情况调整分类及名称：

- a) 一级：泄露将导致企业遭受特别严重经济损失或核心竞争力丧失的商业秘密，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较大经济损失或竞争优势明显减弱的商业秘密，如重要工艺流程、主要客户信息、关键经营数据等；
- c) 三级：泄露将对企业造成一定不利影响的其他商业秘密信息。

8.3 定密管理

8.3.1 定密主体：商业秘密的确定应由产生该信息的业务部门提出申请，经保密委员会审核批准。一级由企业主要负责人或其授权人审批。

8.3.2 定密流程按下列程序实施：

- a) 业务部门识别信息；
- b) 保密委员会审核；
- c) 确定密级和保密期限；
- d) 登记并标注商业秘密。

8.3.3 保密期限：根据商业秘密的时效特性合理确定保密期限。保密期限届满或商业秘密已公开的，应及时解密。

8.3.4 解密条件：出现下列情形之一的，应及时解密：

- a) 信息已公开的；
- b) 信息已失去商业价值的；
- c) 被新技术替代已无保护必要的。

8.3.5 动态管理：商业秘密密级调整（升密、降密、解密）应履行审批程序，并及时更新商业秘密清单和相关标识。

8.4 商业秘密清单

企业应建立商业秘密清单，实行登记、审核与动态管理。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。

8.5 标识管理

企业应在涉密载体上标注密级、保密期限及保密警示标识。标识应清晰、醒目、不易去除。电子文件应采用数字水印、元数据标注等方式进行密级标识。

9 数据保护

9.1 数字化保护措施

9.1.1 企业宜运用互联网、大数据、云计算、人工智能、区块链等手段，推动商业秘密保护数字化转型，大数据处理活动应符合 GB/T 35274 的安全能力要求。

9.1.2 企业应按照 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，全流程执行审批与日志留存。

9.1.3 企业应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。

9.2 电子存证

9.2.1 企业宜采用电子签名、可信时间戳等技术手段，对商业秘密的形成、使用、流转过程进行固定和存证，提升证据固定与取证能力。

9.2.2 区块链存证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。

9.2.3 电子存证内容应包括：商业秘密文件哈希值、存证时间、操作人信息、操作类型等。

9.2.4 企业可借助公证机构办理商业秘密公证存证，提升证据效力。可利用电子存证服务等技术手段，进行商业秘密确权存证。

9.3 网络和信息安全防护

9.3.1 企业应按照 GB/T 22080 建立信息安全管理体系统，部署防火墙、入侵检测、防病毒、数据防泄漏

(DLP)等安全设备,应按照 GB/T 22239 规定的网络安全等级保护基本要求。

9.3.2 涉密网络应与互联网物理隔离或采用经认证的安全隔离设备。

9.3.3 企业应定期开展网络安全风险评估和渗透测试,及时修补安全漏洞。

9.3.4 企业应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。

9.4 远程办公与 AI 应用管理

9.4.1 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,禁止在公共网络环境下处理涉密信息。

9.4.2 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,禁止将涉密信息输入未经授权的公共 AI 平台。

9.4.3 企业应建立 AI 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。

10 物理安全与区域管理

10.1 区域划分

- a) 企业应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。

10.2 区域管控

10.2.1 涉密区域宜与其他工作区域物理隔离,配置门禁系统、视频监控、入侵报警等安全防护设施。

10.2.2 涉密区域入口处应设置明显的警示标识和保密提示。

10.2.3 不同区域之间的人员流动宜符合保密隔离制度要求,核心区域实行双人双锁管理。

10.2.4 外部人员进入涉密区域应经过审批,由专人全程陪同,并登记进出记录。

10.3 物理安全措施

10.3.1 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。

10.3.2 涉密区域的打印、复印、扫描设备应专人管理,操作记录留存备查。

10.3.3 涉密区域宜设置手机存放柜,使用期间禁止携带具有存储功能的个人电子设备进入。

11 合作方与外部管理

11.1 合作方管理

合作开发的商业秘密的权利归属,根据当事人签订的协议确定。协议没有约定或约定不明确的,由当事人协商确定。协商不成的,由实际完成该商业秘密的开发方享有,合同各方均享有商业秘密的使用权,后续改进的商业秘密的权利归属,没有约定的,归属后续改进的开发人。

11.1.1 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,签订保密协议,保密协议应明确:保密信息范围、保密期限、保密义务、违约责任、争议解决方式等条款。

11.1.2 合作进行中,企业应当监督保密协议履行。

11.1.3 合作结束后,应依据保密协议处置保密信息,并出具书面确认。

11.1.4 企业应当保守合作方商业秘密,并遵守相关规定。

11.2 外部信息披露

11.2.1 向外部披露商业秘密应按需披露，遵循最小必要原则，明确披露范围、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、跨境合作、融资上市及并购重组等需要向外部提供商业秘密信息前，应签订保密协议，明确保密责任和义务。

11.2.3 信息披露应经业务部门申请，由商业秘密管理办公室和相关负责人分级审批。

11.3 长三角区域协同

11.3.1 企业涉及长三角区域联合研发、技术转移等活动时，可探索建立跨区域、行业保密协作。

11.3.2 企业可利用长三角区域商业秘密保护协作平台，获取跨地区维权援助和协同保护公共服务。

12 重点场景保护

12.1 员工人员流动

12.1.1 企业应建立离职风险预警机制，对核心涉密人员的离职动向保持关注。

12.1.2 离职前应全面回收涉密资料、门禁卡、密钥等，注销系统权限。

12.1.3 离职面谈应明确告知保密义务、竞业限制要求及泄密法律后果。

12.1.4 对离职员工入职竞争对手的情况，应评估泄密风险，必要时采取法律措施。

12.2 研发环节保护

12.2.1 研发项目立项时应进行商业秘密风险评估，确定保护策略。

12.2.2 研发过程应实行分区隔离管理，不同项目团队间的信息交流应受控。

12.2.3 研发数据应及时备份并存证，实验记录应由专人管理。

12.2.4 涉及外部协作的研发项目，应签订保密协议，明确知识产权归属和保密义务。

12.2.5 后续改进的技术秘密，没有约定的，归属后续改进的开发人享有；技术转让合同履行中后续改进的技术秘密权利归属：

- a) 技术秘密转让合同或实施许可合同履行中一方后续改进的技术成果，根据约定确定其归属。
- b) 没有约定或者约定不明确的，由完成该后续改进的一方享有，其他各方不享有权利。

12.3 涉密活动管理

12.3.1 涉密活动应提前审批，确定参加人员范围，禁止无关人员列席。

12.3.2 涉密活动应在符合保密要求的场所进行，活动前检查有无录音录像设备。

12.3.3 活动材料应编号发放、回收登记，禁止私自复印或拍照。

12.3.4 活动记录文件应标注密级，按涉密文件管理。

12.4 数字化转型

12.4.1 企业上云、使用 SaaS 服务时，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。

12.4.2 数据迁移过程中应采取加密传输，迁移完成后验证数据完整性。

12.4.3 企业应建立数据备份和灾难恢复机制，定期进行恢复演练。

12.5 跨境协同保护

12.5.1 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。

- 12.5.2 企业应与境外合作方签订符合国际惯例的保密协议（NDA），明确适用法律和争议解决方式。
- 12.5.3 跨境数据传输应采用加密通道，传输记录留存备查。

13 风险识别与防控

13.1 风险识别

- 13.1.1 企业可依据 ISO/IEC 27005 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。
- 13.1.2 风险识别范围包括但不限于：人员流动、系统漏洞、物理安全、合作方管理、供应链安全等。
- 13.1.3 企业可借助开展商业秘密保护“事前体检”，全面排查风险隐患。

13.2 风险分级

企业应根据风险发生的可能性和影响程度，将风险划分为高、中、低三个等级，分别制定防控措施：

- a) 高风险：可能导致一级商业秘密泄露，应立即处置；
- b) 中风险：可能导致二级商业秘密泄露，应限期整改；
- c) 低风险：可能导致三级商业秘密泄露或管理混乱，应持续监控。

13.3 风险处置

- 13.3.1 企业应针对识别出的风险制定防控方案，明确责任部门、整改措施和完成时限。
- 13.3.2 企业宜借助保护行业协会等第三方力量，获取专业咨询和合规审查服务。
- 13.3.3 企业应建立供应链安全评估机制，对核心供应商的保密能力进行审查。

13.4 保护路径选择

企业应根据技术特点和市场策略，合理选择商业秘密保护或专利保护：

- a) 技术信息可能丧失先进性或被他人抢先申请专利的，宜申请专利；
- b) 简单、易被反向工程解析的技术信息，宜采用专利保护；
- c) 复杂、不易被他人自行研究且不易被反向工程解析的技术信息，可采用商业秘密保护；
- d) 一项技术可将部分内容申请专利、部分内容作为商业秘密加以保护。

14 应急处置与权利救济

14.1 泄密事件应急处置

- 14.1.1 权利人应制定商业秘密泄密应急处置预案，明确应急响应流程、责任人和处置措施。
- 14.1.2 发现泄密事件后，应立即启动应急预案，采取以下措施：
 - a) 第一时间控制泄密范围，终止信息扩散；
 - b) 启动内部调查，查明泄密原因和责任人员；
 - 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，确定维权策略；
 - e) 必要时向行政机关举报或向公安机关报案。
- 14.1.3 企业宜定期开展泄密应急演练，提升应急处置能力。

14.2 证据收集与固定

14.2.1 企业应注重日常证据留存，包括但不限于：商业秘密权属证明、保密措施证明、商业价值证明等。

14.2.2 发生侵权时，企业应及时收集和固定证据，可采用公证保全、电子存证等方式。

14.2.3 企业可寻求行政机关、维权援助机构的指导和协助。

14.3 权利救济途径

14.3.1 商业秘密权利人可通过以下途径维护自身合法权益：

- a) 民事救济：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》向人民法院提起民事诉讼；
- b) 行政救济：依照《中华人民共和国反不正当竞争法》向市场监督管理部门投诉举报；
- c) 刑事救济：对涉嫌侵犯商业秘密犯罪的，向公安机关报案。

14.3.2 具体的救济程序和要求，依照相关法律法规执行。

14.4 境外维权与应诉

14.4.1 权利人在境外遭受商业秘密侵权的，可通过以下途径维权：

- a) 依据侵权行为地法律提起民事诉讼；
- b) 利用国际仲裁机制解决争议；
- c) 寻求我国驻外使领馆商务处的协助；
- d) 利用国际知识产权组织或贸易协定的争端解决机制。

14.4.2 企业开展海外业务前，应了解目标国家或地区的商业秘密保护法律制度，做好前置风控。

14.4.3 涉及跨境商业秘密纠纷的，可借助长三角区域协同保护机制或专业涉外法律服务机构获取支持。

15 检查与改进

15.1 自查机制

15.1.1 企业应建立商业秘密保护定期自查制度，每年至少开展一次全面自查。

15.1.2 自查内容应覆盖本文件各项要求的落实情况，商业秘密保护自查内容可依据本标准展开。

15.1.3 自查结果应形成书面报告，报送保密委员会审议。

15.2 问题整改

15.2.1 对自查发现的问题，应制定整改方案，明确整改责任、措施和时限。

15.2.2 整改完成后应进行复核验证，确保问题得到有效解决。

15.2.3 对重大隐患应立即整改，必要时暂停相关业务活动。

15.3 持续改进

15.3.1 企业应定期评估商业秘密保护体系的有效性，根据内外部环境变化及时调整保护策略。

15.3.2 企业应关注行业最佳实践和新技术发展，持续优化保护措施。

15.3.3 企业应建立保护工作经验总结和分享机制，促进管理水平不断提升。

15.4 第三方服务

15.4.1 企业可委托第三方专业机构开展商业秘密保护评估评审，获取客观评价和改进建议。

- 15.4.2 企业可利用江苏省商业秘密保护站提供的事前体检、事中合规审查、事后评估评审等服务。
- 15.4.3 鼓励企业参与商业秘密保护创新试点，探索保护新方法、新机制。

参 考 文 献

[1] GB/T 22081 网络安全技术 信息安全控制

[2] 《中华人民共和国反不正当竞争法》

[3] 《中华人民共和国劳动合同法》

[4] 《中华人民共和国数据安全法》

[5] 《中华人民共和国个人信息保护法》

[6] 《中华人民共和国刑法》（侵犯商业秘密罪相关条款）

[7] 《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》

[8] 《最高人民法院、公安部关于修改侵犯商业秘密刑事案件立案追诉标准的决定》

[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》
