ICS 03.100.01
CCS A 01

MR-XXXX

# 中华人民共和国市场监管行业标准

MR/TXXXXX—XXXX

# 企业商业秘密保护管理规范

Specification for enterprise trade secret protection

（征求意见稿）

2026 年 3 月 2 日

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

国家市场监督管理总局　　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。

本文件由国家市场监督管理总局提出并归口。

本文件起草单位：国家市场监督管理总局认证认可技术研究中心。

本文件主要起草人：XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX。

# 引　言

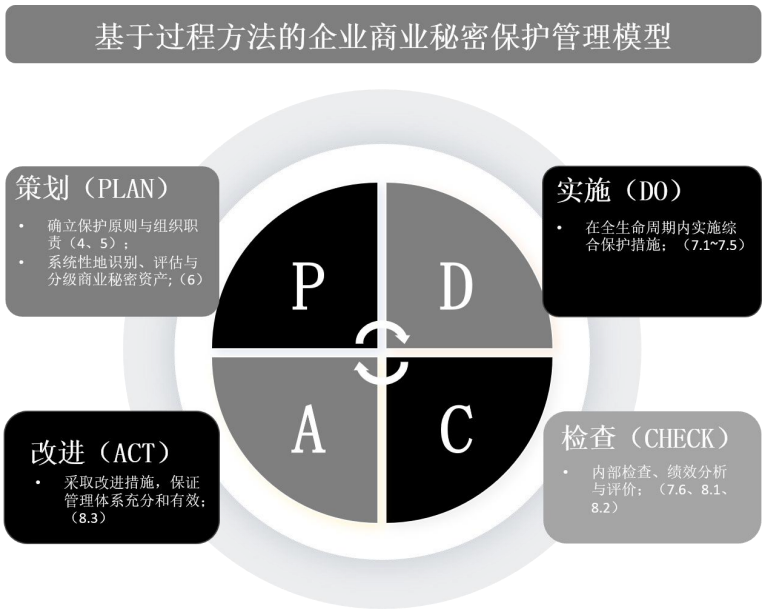
## 0.1　概述

商业秘密是企业创新发展与社会新质生产力发展的重要支撑，是维护市场公平竞争秩序、激发经营主体创新活力的关键环节。

本文件提供了基于过程方法和风险思维的商业秘密保护管理方法，指导企业建立、实施、运行、评审和改进商业秘密保护体系，旨在降低商业秘密在处理、存储、传输及共享环节的泄露风险，为企业创新发展筑牢安全屏障。

## 0.2　过程方法

图 1 表明了本标准第 4 章至第 8 章是如何构成 PDCA 循环的。




本文件采用了基于过程的方法：

a) 策划（P）：确立保护原则与组织职责（第 4、5 章），并系统性地识别、评估与分级商业秘密资产（第 6 章），作为整个管理体系的基础与输入；

b) 实施（D）：依据策划结果，在全生命周期内实施涵盖人员、物理、技术、外部协作及应急维权等的综合保护措施（第 6、7 章）；

c) 检查（C）：根据保护方针、目标、要求和策划的活动，通过内部检查、事件溯源与绩效监测等方式（8.1、8.2），对商业秘密保护过程及实施效果进行监测和评价，验证保护措施的执行有效性，识别偏离、漏洞与潜在风险，并报告结果；

d) 改进（A）：根据检查结果，采取纠正与预防措施（8.3），更新保护策略、优化管控流程，持续改进商业秘密保护管理体系及其绩效，确保体系持续充分、有效并不断完善。

## 0.3 基于风险的思维

风险控制与风险评价是防范泄露商业秘密、提升商业秘密保护效能的基础性工作，贯穿商业秘密全生命周期管理的各个环节，为保护商业秘密提供导向与保障。

# 企业商业秘密保护管理规范

## 1 范围

本文件规定了企业商业秘密保护管理的总则、组织管理、商业秘密的识别与分级、保护措施、绩效评价与改进等要求。

本文件适用于企业商业秘密保护。企业根据自身的行业特点、业务模式等实施商业秘密保护，可在全部经营活动中实施，也可在特定阶段或特定部门内实施。

## 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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 29490 企业知识产权合规管理体系 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 secrets**

不为公众所知悉、具有商业价值并经企业采取相应保密措施的技术信息、经营信息等商业信息。

**注1：**技术信息包括与技术相关的结构、原料、组分、配方、材料、样品、样式、职务新品种繁殖材料、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2：**经营信息包括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（名称、地址、联系方式以及交易记录、交易习惯、交易意向、内容等）、数据等信息。

3.2

**涉密载体 secret-related 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介质。

**注：**包括磁性介质、光盘、U盘、硬盘、服务器等电子存储介质及包含商业秘密信息的纸质、设备、仪器、产品等物理性载体。

## 4 总则

### 4.1 全生命周期管理

企业商业秘密保护覆盖商业秘密的全生命周期，包括商业秘密从产生到销毁的各个阶段。

### 4.2 全员参与

企业各级人员重视和积极参与商业秘密保护工作。

### 4.3 平衡与协同

企业根据商业秘密分级情况，采取相应保护措施，在商业秘密保护与利用、员工权益与企业利益、风险控制与管理成本之间达到平衡。

## 5 组织管理

### 5.1 机构、部门与人员

5.1.1 企业的最高管理者应对商业秘密保护担负领导作用。

5.1.2 企业可设立商业秘密保护部门或依托相关部门开展商业秘密保护工作，配备专/兼职保密人员。

5.1.3 商业秘密保护部门和保密人员应履行以下职责，包括但不限于：

——建立和实施商业秘密保护制度；

——识别和管理商业秘密；

——组织商业秘密保护宣传、培训；

——监督、检查商业秘密保护的实施，并持续改进；

——应对侵犯商业秘密行为。

5.1.4 企业各部门负责人为本部门商业秘密保护第一责任人，履行以下职责：配合完成本部门商业秘密的识别与分级，落实本部门商业秘密的保护措施，及时报告本部门的泄密风险和事件。

### 5.2 制度与流程

企业应制定商业秘密安全管理制度，包括但不限于：

——商业秘密从产生到销毁的各阶段；

——涉密区域、载体、岗位、人员。

——商业秘密的识别、分级与动态更新机制；

——员工管理（涵盖：入职、履职、离职等）管理；

——涉密载体与区域的物理安全控制与销毁流程；

——技术防护（权限、日志、存储、使用、网络、对外提供、脱密等）管理；

——外部协作活动中的保密协议与过程管控；

——应急响应预案、事件处置流程；

——管理制度与流程的持续改进机制。

## 6 商业秘密的识别与分级

### 6.1 商业秘密的识别

6.1.1 商业秘密识别应考虑：

a) 价值：商业秘密在企业生产经营中带来的直接经济价值和商业秘密带来的竞争优势、声誉形象等间接经济价值；

b) 影响程度和影响范围：商业秘密泄露对企业市场竞争优势、运营安全、声誉形象的影响程度及商业秘密泄露可能对企业的损害范围（影响企业全局业务、多个业务线或局部业务）；
c) 替代成本：商业秘密被替代所需要投入的资金成本与时间周期；
d) 使用范围：知悉或可能知悉的主体数量；
e) 强制性要求：是否涉及国家秘密、出口管制、行业监管等合规要求。

6.1.2 企业开展商业秘密识别应按照以下步骤:

a) 信息梳理与筛选：通过部门访谈、流程分析、信息系统盘点等方式，梳理生产经营活动中形成和控制的信息；依据商业秘密构成要件，从信息中筛选确定商业秘密信息；

注：必要时，企业可委托第三方机构（如知识产权服务机构、律师事务所、专业咨询公司）在签订完备的法律协议、严控保密义务后对商业秘密信息进行筛选。

b) 商业秘密信息的分类：分类方式包括但不限于：
——按照内容分类：分为技术信息与经营信息等；
——按照经济价值：分为高价值商业秘密与一般价值商业秘密等；
——按照业务领域：分为研发数据、生产数据、营销数据、财务数据等；
——按照描述对象：分为技术资料、交易数据、供应商信息、管理数据等；
——按照生命周期：分为信息的产生、存储、流转、加工、传输、归档和销毁等环节；
c) 建立清单：根据分类确定涉密载体、责任部门、保密措施等，编制形成企业商业秘密清单。

## 6.2 商业秘密的分级

6.2.1 企业应根据商业秘密的商业价值及其一旦泄密可能造成的危害程度，建立分级标准：

a) 具有极高商业价值，泄密会导致企业丧失核心竞争力，造成重大经济损失，导致企业生存危机或严重触犯法律法规的商业秘密，定为核心商密；
b) 具有较高商业价值，泄密会显著削弱企业市场竞争力，造成较大经济损失，对企业核心业务造成持续影响的商业秘密，定为普通商密。

注1：需要时，可增加一般商密，具有一定商业价值，泄密可能导致企业运营效率降低，造成一定的经济损失，但不会对企业核心竞争力和长期经营造成影响的商业秘密，定为一般商密。

注2：当一项商业秘密符合多个不同级别规则特征的，按照‘就高原则’确定级别。

6.2.2 根据分级标准形成《企业商业秘密分级清单》，由商业秘密保护部门牵头，组织内部相关部门对清单进行评审，经过企业最高管理者或授权人员批准发布。

6.2.3 企业应建立商密级别的动态更新机制：

a) 企业应定期对《企业商业秘密清单》进行评估、更新、评审与发布；
b) 当发生但不限于以下情形时，企业应立即对商业秘密级别重新评估和调整：
——商业秘密价值发生显著变化时；
——核心技术或技术环境发生重大变化时；
——法律法规或行业监管要求发生变更时；
——发生泄密事件导致商业秘密扩散或价值受损时；
——多个同级商业秘密信息汇聚，衍生或产生更高价值商业秘密信息时。

# 7 保护措施

## 7.1 员工管理

### 7.1.1 入职管理

7.1.1.1 针对有工作经历的拟入职人员，企业应重点审查其是否与原单位签署了保密协议、竞业限制协议等法律文件，同时要求该人员书面承诺不将在原单位知悉的任何商业秘密用于本职工作，并签署具有法律效力的承诺书。

7.1.1.2 企业应与新入职人员签署保密协议，明确界定商业秘密的范围、保密期限、双方的权利与义务以及违约责任等。对于高级管理人员、高级技术人员等能够接触到企业核心商业秘密的重点岗位人员，应签署竞业限制协议，明确约定竞业限制的具体范围、期限、违约责任、补偿费的具体数额及支付方法等。

7.1.1.3 企业应对新入职人员建立基本的账号与权限管理机制，确保对商业秘密信息的访问受控。应遵循“最小必要”原则分配权限，确保新入职员工仅拥有完成本职工作所必需的系统访问与操作权限.

7.1.1.4 企业应对新入职人员进行系统的商业秘密保密培训和教育，涵盖企业的商业秘密管理制度、保密义务的具体内容、潜在法律风险以及内部保护措施，以增强入职员工的保密意识。

### 7.1.2 履职管理

7.1.2.1 企业可将商业秘密保护培训纳入年度培训计划，对在职员工定期开展商业秘密保密培训和保密教育，持续提升员工的保密意识与保密技能。

7.1.2.2 企业建立常态化的监督考评机制，定期对员工遵守商业秘密管理制度的情况及参与培训的效果进行考察评估。对违反商业秘密管理规定的行为，其处罚结果应形成书面文件，并在企业内部进行通报，以达到警示和教育的目的。

### 7.1.3 离职管理

7.1.3.1 企业应明确告知离职人员其离职后应承担的保密义务、竞业限制义务（如涉及）以及违反相关规定可能导致的法律责任，形成书面文件并由离职员工签字确认。

7.1.3.2 企业应及时收回离职人员的相应系统权限，包括但不限于门禁卡、邮箱账号、内部系统账户、数据库查询权限等，并注销或变更相关密码；并要求其移交所有原始的涉密载体，如文件、图纸、移动存储设备、工作电脑等，配合企业做好工作交接。

7.1.3.3 企业应对离职员工交还的涉密载体（不限于工作电脑、存储设备）等进行完整性检查，重点核查是否存在数据篡改、异常拷贝、非授权外发等行为；核查过程中如发现存在涉嫌侵害商业秘密的行为，应立即采取措施保护证据，必要时采取维权措施。

7.1.3.4 对于接触核心商密的员工，应在其离职时启动离职审计，审计内容可包括其在职期间的资料访问记录、客户联络行为、业务操作合规性等，并可根据实际情况设定脱密期限。

7.1.3.5 对受竞业限制约束的离职员工，企业可通过公开渠道、客户反馈、市场信息等方式，定期了解其任职情况，判断是否存在违反竞业限制协议或侵害商业秘密的行为。

## 7.2 物理安全

7.2.1 企业应划定专门的涉密区域用于保存和处理涉密载体，并根据商业秘密等级对涉密区域及载体进行分级管理：

a) 普通商业秘密保护应符合：

——涉密区域应采取门、锁等物理措施与普通区域进行隔离，控制人员进出；

——应根据商业秘密级别和业务需要，对涉密区域进行标识，并明确授权访问的人员名单；

——应对进入涉密区域的访客，应进行登记并由内部人员陪同；

b) 核心商密保护还应符合：

——在涉密区域工作的人员，应要求其签署专门的保密协议，并限制其无授权的录像、摄像等影音记录设备使用；

——存储核心商密的区域，宜采用电子门禁（如刷卡、密码）进行访问控制，并可考虑设置接待区，避免外部人员直接进入核心区域。

7.2.2 企业应对涉密载体进行标识和基础管理：

a) 涉密载体（如文件柜、存储设备等）应进行标识（如“商业秘密”字样），并登记在册；

b) 涉密载体的借用、携带外出应经过责任人审批并进行记录；

c) 涉密载体销毁前，应经相关负责人确认，并采用碎纸、消磁或格式化等适当方式确保信息不可恢复，宜保留销毁记录。

7.2.3 企业应建立基本的监督机制。

a) 普通商业秘密保护应符合：

——应定期（如每季度或每半年）对涉密区域的访问权限清单和物理防护措施的有效性进行检查和复核；

——应安全保存对涉密区域、载体的访问与操作记录，以确认满足最小化授权机制，及时发现违规行为；

b) 核心商密保护还应在核心商密涉密区域宜配备视频监控或定期巡检，为安全事件提供回溯支持。

## 7.3 技术防护

7.3.1 企业应对能够处理商业秘密的信息系统建立基本的账号与权限管理机制，确保对商业秘密信息的访问受控：

a) 普通商业秘密保护应符合：

——企业应制定并执行系统账号的申请、审批、分配与回收流程。员工岗位或职责变动时，应及时调整或撤销其相关系统权限；

——应遵循“最小必要”原则分配权限，确保员工仅拥有完成本职工作所必需的系统访问与操作权限；

——系统应具备基本的身份鉴别功能（如用户名/口令登录），应配置登录失败锁定、会话超时自动退出等安全策略；

——应明确核心商业秘密数据处理权限的审批责任人，并保留权限分配与变更的记录；

b) 核心商密保护还应符合：对存储或处理核心商业秘密的系统，其账号口令应具备一定复杂度要求（如长度、字符组合），并定期更换。

7.3.2 企业应对其商业秘密信息系统的重要操作进行日志记录，以支持事后的安全审计与事件追溯：

a) 普通商业秘密保护应符合：

——商业秘密信息系统应能够记录用户登录与退出、商密数据的创建、修改、批量导出与删除等关键操作日志；

——应采取措施防止日志被非授权访问、恶意篡改或删除；

——关键操作日志的留存时间应不少于 90 天，以满足基本的事件追溯需求（企业可根据法律法规或实际风险，确定更长的保留期限；

b) 核心商密保护还应符合：

——企业应指定专人（或岗位）负责定期（如每季度或每半年）审阅日志，检查是否存在异常或违规操作迹象；

——涉及核心商业秘密数据的关键操作（如访问、修改、外发）日志，其留存时间应延长至 180 天或以上，并宜进行定期备份。

7.3.3 企业应对存储于商业秘密信息系统中的商业秘密信息采取基本的安全存储措施，防止信息泄密露与篡改：

a) 普通商业秘密保护应符合：

——应采用访问控制、密码技术等措施进行安全存储，防止被非授权访问和窃取；

——商业秘密信息应进行定期备份；

b) 核心商密保护还应符合：核心商业秘密应集中存储于可控的服务器或专用存储设备中，避免大量存储于员工个人终端设备（如笔记本电脑、移动硬盘等）。

7.3.4 企业应对商业秘密数据的使用过程进行基本管控，在保障业务效率的同时，降低使用环节的泄密风险：

a) 普通商业秘密保护应符合：

——在不影响员工正常的文档编辑阅读、数据处理、数据交换、出差和在外办公为前提，对商业秘密数据进行管理和控制。

——商业秘密数据应在创建和存储时应自动加密，应依据“最小权限原则”，对数据的操作行为进行技术管控，禁止或限制复制、打印、截屏、另存为等可能导致内容泄露的操作；

——应在使用商业秘密数据的终端屏幕上显示自定义位置、格式和透明度的水印，以防范通过拍摄屏幕等方式导致的信息泄露；

b) 核心商密保护还应在上述基础上，对核心商业秘密信息采用区块链等防伪造、防篡改技术进行存证，形成可信的电子证据，确保在发生安全事件时能够进行有效溯源和责任认定。

7.3.5 企业应建立销毁安全机制：

a) 应建立商业秘密数据销毁制度，明确销毁流程和责任主体；

b) 应采用数据擦除或物理销毁等不可恢复的方式，安全处置存有商业秘密的存储介质。

7.3.6 企业应建立网络安全机制：

a) 根据业务流程、网络部署和安全风险等情况，合理划分网络系统安全域，明确商业秘密数据传输场景与保护措施；

b) 采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，保障商业秘密数据传输过程中的机密性和完整性；

c) 运行商业秘密信息系统的网络中，未经授权不应使用带有网络嗅探功能（包括抓包、监听、数据包回放分析等）的工具或设备；

d) 不应租用无相关资质的第三方服务商提供的网络应用服务传输核心商业秘密数据，包括外部邮件服务、外部基于云计算技术的服务、即时通信服务等。

7.3.7 企业应建立对外提供信息安全机制：

a) 制定商业秘密对外提供的评估和审批流程，明确商业秘密提供的范围、类别、条件、授权等；
b) 使用商用密码加密等安全技术，对外发的商业秘密数据内容进行安全保护，且对商业秘密数据知悉范围和权限进行控制；
c) 应在商业秘密对外提供前，签订合作合同和保密协议，明确数据安全保护条款，包括合作的数据范围、数据用途、期限和违约责任等；
d) 商业秘密数据提供涉及数据出境时，应按照国家相关规定和相关标准的要求执行；
e) 核心商业秘密应由两个及以上相关人员审批通过后才可外发；
f) 对外提供商业秘密时，应核验数据接收方的身份。

## 7.4 外部协作管理

7.4.1 在开展对外技术合作、供应商合作等各类外部协作事项前应识别相应密级等，并保留涉及商业秘密的成文信息。

7.4.2 在采购、销售、参展等对外商务合作中，企业应采取下列措施，包括但不限于：

a) 在商务谈判前或提供商业秘密前，与对方签订保密协议，明确保密条款；
b) 在参展等商务活动过程中涉及商业秘密的，应对参展产品或技术采取相应防护手段，防止他人未经授权的接触、拆解、复制或者窃取；
c) 对保密协议履行过程中商业秘密的履行、违约、披露、泄密等情况进行日常管理。

7.4.3 在委托开发、合作开发、定作、加工、承揽等对外技术合作中，企业应采取下列措施，包括但不限于：

a) 了解合作方的商业秘密管理能力；
b) 在技术合作中采取措施防止侵犯他人商业秘密，必要时保存商业秘密权利人承诺其商业秘密不侵犯第三人的声明；
c) 约定共同开发、改进或二次开发中涉及商业秘密的内容与所有权归属，必要时可单独就保密内容签订保密协议。

7.4.4 聘任或委托外聘专家、顾问、翻译、律师等可能接触商业秘密的外部人员，宜做背景调查，并签订保密协议或保密条款、或保密承诺书。

7.4.5 接受外部单位开展的尽职调查、检查、审计、评估等活动前，应与其签订保密协议或保密条款。

7.4.6 涉及商业秘密的会议或其他活动，应采取但不限于下列保密措施：

a) 限定参加人员的范围，指定参与涉密事项的人员；
b) 告知参加人员保密要求，必要时签订保密承诺书；
c) 对商业秘密涉密文件、资料进行控制：
——确定发放范围，做好发放登记；
——重要涉密文件资料应有明显保密标识和会后回收标识；
——休会或会议结束时，及时收回清点、登记。

7.4.7 外部协作保密协议应明确保密要求，约定保密内容、范围、权利义务、保密责任、违约责任，对涉及商业秘密的权利归属和使用作出约定。

## 7.5 应急管理

### 7.5.1 应急管理组织

企业宜成立由最高管理者牵头的商业秘密泄密应急管理小组，负责应急事件决策与资源调配。组建应急执行组织，负责应急预案制定、演练组织和应急事件处置、证据收集与固定及外部资源协调和采取维权行动。

### 7.5.2 应急事件分级

7.5.2.1 企业应根据行业特性和商业秘密分类分级标准，以及商业秘密范围、数量和所造成影响等因素确定应急事件的分级标准，一般可分为重大事件、较大事件和一般事件。

7.5.2.2 企业应根据应急事件的等级，明确事件处置责任分工、工作流程和处置措施。

### 7.5.3 应急预案与演练

7.5.3.1 企业应制定商业秘密泄密事件的应急响应预案，预案内容应包括：

a) 充分考虑可能出现商业秘密威胁事件的各类场景，包括但不限于商业秘密泄露(丢失)、商业秘密被篡改、商业秘密被损毁、数据违规或违约使用、商业秘密被披露等；
b) 根据场景制定防止损失扩大的保护措施；
c) 商业秘密泄密事件的调查、确认和影响评估，查明事件原因、过程和责任人；
d) 证据搜集、固定；
e) 内部问责和外部维权。

7.5.3.2 宜组织定期开展应急预案演练，根据演练结果情况评估应急预案的有效性，并进行修改完善。

7.5.3.3 培训和引导员工对泄密保持警觉，发现泄密迹象及时报告。

### 7.5.4 应急事件处置

7.5.4.1 出现商业秘密泄露时，应急管理组织应立即评估商业秘密事件等级，并立即启动相应的应急预案。

7.5.4.2 商业秘密威胁事件得到控制后，应尽快有针对性地完善保密措施，防止再次发生商业秘密威胁事件。

## 7.6 维权

7.6.1 企业在发现商业秘密被侵犯的迹象、线索时，应搜集并整理下列证据性材料：

a) 企业是该商业秘密的权利人的证据：
——泄密信息的具体内容、载体；
——泄密信息为一般公众不知悉或者无法轻易获得的证明；
——已采取的保密措施。
b) 合理表明该商业秘密被侵犯的初步证据：
——泄密人员能够接触秘密信息且被侵权信息与该秘密信息实质相似的初步证据；
——泄密人员相关信息：包括签订劳动合同/保密协议、参与的保密培训、具体工作职责等信息；
——可能的泄密途径；
c) 该商业秘密被侵犯的损害事实：
——侵权行为具体表现（如非法获取、非法披露、非法使用等）；
——被侵权所受的损失或侵权行为所获得收益；

——主张法定赔偿的参考因素及其证据。

7.6.2 宜制定证据固定操作规范，对于电子证据、纸质证据、人员证据、第三方证据明确固定流程和标准，确保证据收集的完整性与有效性。

7.6.3 企业应结合泄露事件所造成的相应影响和所收集的证据，选择一项或多项维权方式：

a) 向市场监督管理部门举报；
b) 向公安机关报案；
c) 向仲裁机构申请仲裁；
d) 向人民法院提起民事诉讼等。

7.6.4 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。

7.6.5 企业在依法维权过程中，应防止商业秘密的二次泄露。

## 8 绩效评价与改进

### 8.1 内部检查

8.1.1 企业应制定、实施商业秘密保护情况的检查方案，内容包括时间、地点、人员、方法、检查内容等，检查内容包括但不限于：

a) 企业商业秘密组织与机构的履职情况；
b) 商业秘密保护制度建立及完善情况；
c) 商业秘密识别与分级的适宜性；
d) 商业秘密保护措施运行情况。

8.1.2 检查中应重点关注：

a) 是否发生或潜在存在商业秘密披露、泄密的情况或风险；
b) 是否发生或潜在存在侵犯商业秘密行为或风险；
c) 前次检查中发现问题的改进情况等。

### 8.2 分析与评价

企业应根据获得的适当的信息进行绩效分析并形成结果，利用分析结果评价：

a) 涉及商业秘密保护有关资源的充分性；
b) 商业秘密保护制度的适宜性；
c) 商业秘密保护措施的有效性；
d) 商业秘密安全保护工作改进的需求。

### 8.3 改进

8.3.1 企业应对出现商业秘密泄露事件及问题、隐患进行调查与评价，分析原因，确定和实施相应措施，并对所采取措施的有效性进行评审。企业应保留相关改进的成文信息。

8.3.2 企业应持续改进商业秘密保护管理工作的适宜性、充分性和有效性。

# 参 考 文 献

[1] GB/T 18894－2016 电子文件归档与电子档案管理规范

[2] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国反不正当竞争法（2025年修订）

[3] 中华人民共和国全国人民代表大会常务委员会.中华人民共和国民法典：中华人民共和国主席令第45号.2020年

[4] 最高人民法院.《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》：法释〔2020〕7号.2020年

[5] 最高人民检察院，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》：高检发〔2020〕15号.2020年

[6] 最高人民法院，最高人民检察院.《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件适用法律若干问题的解释》：法释〔2025〕5号.2025年