

# DB4403

深 圳 市 地 方 标 准

DB4403/T 461—2024

## 科研机构商业秘密保护管理规范

Management specification for protection of trade secrets of science  
and technology research organizations

2024-06-25 发布

2024-07-01 实施

深圳市市场监督管理局 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 .....	3
5 商业秘密组织管理 .....	3
6 商业秘密制度管理 .....	4
7 商业秘密保护宣传与培训管理 .....	4
8 商业秘密资产确认 .....	5
8.1 实施要求 .....	5
8.2 商业秘密载体盘点 .....	5
8.3 商业秘密载体归档 .....	6
8.4 商业秘密电子存证 .....	6
9 商业秘密资产内部保护 .....	8
9.1 涉密岗位管理 .....	8
9.2 涉密人员管理 .....	8
9.3 涉密文档管理 .....	10
9.4 涉密系统管理 .....	11
9.5 涉密区域管理 .....	13
10 商业秘密资产外部保护 .....	14
10.1 信息公开 .....	14
10.2 商务活动 .....	14
10.3 委外服务 .....	14
10.4 科技成果转化 .....	14
11 检查与改进 .....	15
12 应急与维权 .....	15
参考文献 .....	17

## 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》给出的规则起草。

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。

本文件由深圳市市场监督管理局提出并归口。

本文件起草单位：深圳高智量知识产权代理有限公司、深圳市市场监督管理局、深圳市光明科学城知识产权公共服务中心、广东智诚知识产权研究院、深圳市标准技术研究院、深圳湾实验室、深圳大学知识产权研究所、深圳市公标知识产权鉴定评估中心。

本文件主要起草人：李飞、洪隽、李富山、陈建民、朱谢群、彭建勋、吴良卫、潘文欢、曹威、刘莹莹、王向东、冼志林、邓光昀、邓映均、谭丽、刘诚、唐立、张焱、王磊、代维伟、许宗强。

# 科研机构商业秘密保护管理规范

## 1 范围

本文件规定了科研机构商业秘密保护管理的总体要求、商业秘密组织管理、制度管理、保护宣传与培训管理、资产确认、资产内部保护、资产外部保护、检查与改进、应急与维权的要求。

本文件适用于科研机构在研发、科技成果转化、日常经营管理等过程中的商业秘密保护管理。法定机构、协会等组织的商业秘密保护管理可参照本文件执行。

## 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 22239—2019 信息安全技术 网络安全等级保护基本要求

SF/T 0076—2020 电子数据存证技术规范

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**科研机构** science and technology research organization

以自然科学与技术研发为核心业务，有明确的职能定位、研发布局，拥有研发人才队伍，具备研发资源条件，能够有组织、系统性、持续性开展研发活动的组织机构。

注：科研机构是政府、企事业单位或社会力量依法依规设立的法人机构，包括高等学校、研究院所等。

[来源：GB/T 43803—2024，3.1，有修改]

### 3.2

**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：技术信息为与技术有关的结构、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2：经营信息为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，其中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。

[来源：DB4403/T 235—2022，3.1]

### 3.3

**商业秘密载体** trade secret carrier

以文字、数据、符号、图形、图像、声音等方式记载商业秘密（3.2）信息的纸介质、光介质、电磁介质等各类物品。

### 3.4

**涉密人员** secret-related personnel

在工作中能够产出、接触、使用、掌握商业秘密（3.2）的科研机构（3.1）工作人员以及其他负有保密义务的第三方人员。

### 3.5

**涉密岗位** secret-related position

在工作中能够产生、经管或者经常接触、知悉商业秘密（3.2）事项的岗位。

### 3.6

**涉密部门** secret-related department

在工作中能够产出、接触、使用、掌握商业秘密（3.2）的科研机构（3.1）内部部门。

3.7

**涉密区域 secret-related area**

在工作中制作、存储、保管商业秘密载体（3.3）的场所。

注：包括科研机构园区、厂房、车间、实验室、办公室、保密室、档案室、机房等。

3.8

**元数据 metadata**

描述电子文件和电子档案的内容、背景、结构及其管理过程的数据。

[来源：GB/T 18894—2016, 3.3]

3.9

**归档 file archive**

将具有保存价值且办理完毕的文件及其元数据、管理权限向档案保管部门提交的过程。

3.10

**备份 backup**

将电子文件的全部复制或转换到存储载体或独立的系统上。

3.11

**封存 seal up for safekeeping**

将电子文件的正本或原件转换到存储载体或独立的系统上，并且不再进行任何更改变动。

3.12

**电子数据存证 digital evidence preservation**

通过互联网向科研机构（3.1）提供电子数据证据保管和验证的服务。

[来源：SF/T 0076—2020, 3.1, 有修改]

3.13

**电子数据存证服务提供者 digital evidence preservation service provider**

提供电子数据存证（3.12）服务的机构或组织。

[来源：SF/T 0076—2020, 3.2]

3.14

**电子数据存证平台 digital evidence preservation platform**

由电子数据存证服务提供者（3.13）向使用者以网站、应用程序和编程接口等形式提供电子数据存证（3.12）服务的软件或系统。

[来源：SF/T 0076—2020, 3.4]

3.15

**可信时间标识 trusted timestamp**

唯一的标识某一刻时间的字符序列。

注：该标识不仅可以标识出行为的发生时间，还可以通过时间的先后顺序构建带时序的证据链条。

[来源：SF/T 0076—2020, 3.5]

3.16

**区块链 blockchain**

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[来源：GB/T 37043—2018, 2.5.8]

3.17

**哈希值 hash value**

计算机科学中一种从任何一种资料中建立小的数字的方法，通常用一个短的随机字母和数字组成的字符串来代表，在电子数据取证领域常用作校验数据的完整性。

3.18

**商业秘密存证原件 original files for trade secret evidence preservation**

科研机构（3.1）实际提交至电子数据存证平台（3.14），用以实际进行存证的原始档案。

## 3.19

**存证凭证 evidence preservation certificate**

由电子数据存证服务提供者（3.13）核发，可作为存证保全结果的证明文件。

## 3.20

**商业秘密资产 trade secret asset**

通过确认和有效保护，能够持续发挥作用并且为权利人带来经济利益的非公开商业信息权益。

## 4 总体要求

4.1 科研机构应坚持“管理部门指导监督、自主管理、依规保护”的商业秘密保护管理原则。

4.2 科研机构应明确最高管理者为商业秘密保护的第一责任人，将商业秘密保护管理纳入整体规划，并制定商业秘密保护管理的方针和目标，通过规划、实施、检查及持续改进商业秘密保护管理体系，将商业秘密保护管理措施贯彻到科研机构经营活动中，包括但不限于科研、商业合作、生产、销售、采购、财务、人事、行政，确保制定的相关措施与科研机构自身实际发展水平和发展战略相匹配。

4.3 科研机构应平衡商业秘密安全、管理效率、管理成本三者之间的关系，在不抵触其他管理制度的条件下，制定符合科研机构需求的商业秘密管理制度。涉及属于国家秘密范围的，还应遵守相关法律法规的规定。

4.4 科研机构应建立合法合规的管理文化，重视无形资产价值，致力于建立行业间的公平竞争秩序，引领并发挥正面的示范作用。

4.5 科研机构实施商业秘密保护管理应有相应的计划文件、规范文件、程序文件及管理表单。

## 5 商业秘密组织管理

5.1 科研机构最高管理者应具备商业秘密管理意识，且通过以下方面实现对商业秘密管理体系的领导与管理：

- a) 建立商业秘密管理方针和目标，且与国家法律、政策、行业环境及科研机构战略相一致；
- b) 保障投入具体且有效的资源，保持商业秘密管理体系稳健运行；
- c) 将商业秘密管理要求整合到科研机构的业务流程中；
- d) 要求工作人员建立并加强商业秘密保护意识；
- e) 管理并支持工作人员为商业秘密管理体系的实施持续努力；
- f) 促进商业秘密管理体系持续精进改善；
- g) 维护科研机构商业秘密资产合法权益。

5.2 科研机构应设立商业秘密管理领导部门，由科研机构最高管理者担任总负责人，各部门最高管理者担任该部门第一负责人。商业秘密管理领导部门的成员由科研机构最高管理者依据组织架构或业务现况，指派业务部门主管或由具备商业秘密管理相关职能（如法务、人事、信息安全、知识产权等）的部门主管担任。其职责包括但不限于：

- a) 贯彻落实国家有关商业秘密保护的法律法规和规章；
- b) 贯彻科研机构的商业秘密管理方针、政策、决定和目标；
- c) 负责科研机构商业秘密管理体系的制定、发布、管理、实施和改善；
- d) 持续监控科研机构内部与外部的商业秘密侵害风险；
- e) 明确商业秘密管理领导部门成员和各业务部门商业秘密管理人员的工作职责；
- f) 定期召集商业秘密管理工作会议，梳理和盘点研发与经营过程中形成的商业秘密，促进商业秘密管理体系的持续改进；
- g) 监督、检查商业秘密管理工作的贯彻落实情况；
- h) 对各部门的商业秘密管理工作进行评核并予以奖惩；
- i) 指导开展商业秘密管理的宣传与培训工作；

- j) 积极争取政府或其他外部单位的协同支持；
- k) 组织、协调泄密事件的查处和应急管理，并采取补救措施。

5.3 科研机构应指派专门的商业秘密管理执行人员或工作小组，或由各个部门遴选具有商业秘密管理职能的人员，具体开展商业秘密管理工作。其职责包括但不限于以下事项：

- a) 贯彻科研机构商业秘密管理制度各项规定与程序；
- b) 承担商业秘密管理领导部门赋予的任务，并落实执行；
- c) 定期向商业秘密管理领导部门汇报工作执行成果；
- d) 针对科研机构商业秘密管理制度实施结果，提出改善建议或解决方案；
- e) 负责确认商业秘密资产，并执行相应的保护措施；
- f) 妥善保存商业秘密管理过程中的各项实施记录；
- g) 协助其他人员建立保密观念及给予商业秘密保护工作指导；
- h) 持续接受商业秘密管理专业知识与技能培训，确保足以胜任科研机构管理要求；
- i) 及时向商业秘密管理领导部门通报科研机构内部或外部的商业秘密泄密风险或预警提示；
- j) 针对可能涉嫌侵犯商业秘密的行为或案件，协助进行证据整理与调查工作；
- k) 完成商业秘密管理相关的宣传或推广任务。

5.4 已有保密体系的科研机构宜在原有保密体系基础上建立商业秘密管理体系，相关制度、人员架构宜视情况优化复用或共用，实现秘密管理最小化原则。

## 6 商业秘密制度管理

6.1 科研机构应制定、发布、实施和保存商业秘密管理制度文件，包括但不限于：

- a) 商业秘密管理的目的、目标、方针、适用范围、定义、策略和原则；
- b) 商业秘密管理的组织架构、职责与分工、年度工作计划；
- c) 商业秘密管理的培训实施；
- d) 涉密人员和涉密部门的管理，包括责任与奖惩；
- e) 商业秘密载体的管理；
- f) 实验室和实验数据的管理；
- g) 专利与商业秘密协同管理；
- h) 核心供应商的管理；
- i) 客户专项的管理；
- j) 涉密系统的管理；
- k) 涉密区域的管理；
- l) 商业秘密管理的监督考核机制；
- m) 商业秘密泄密事件应急处理机制。

6.2 科研机构的商业秘密管理制度宜以商业秘密管理手册的形式保存，并在科研机构内部进行正式公示与发布。

6.3 科研机构应每年定期检查并视情况修订和完善商业秘密管理制度。

## 7 商业秘密保护宣传与培训管理

7.1 科研机构开展商业秘密保护宣传与培训工作，可采取的方式包括但不限于：

- a) 发放保密手册或商业秘密管理手册；
- b) 定期举办商业秘密保护培训课程；
- c) 编制、印发商业秘密保护宣传资料；
- d) 在办公场所内张贴宣传标语、播放宣传视频；
- e) 举办商业秘密保护相关研讨会议活动；
- f) 利用科研机构或其他媒体平台进行宣传。

7.2 科研机构应对涉密人员开展商业秘密保护与保密培训，以确保涉密人员明白下列商业秘密保护知



- 识，遵守商业秘密保护的要求，培养商业秘密保护重要观念，培训内容包括但不限于：
- a) 商业秘密的定义与重要性；
  - b) 商业秘密属于科研机构的职务成果；
  - c) 科研机构商业秘密资产的识别与合法使用；
  - d) 泄露或侵害科研机构商业秘密的途径和行为；
  - e) 侵害商业秘密可能承担的法律风险；
  - f) 商业秘密司法判例；
  - g) 科研机构商业秘密管理制度的实施内容；
  - h) 其他与保密义务、保密范围、保密行为有关的内容。
- 7.3 科研机构可针对不同单位、职务或权限的人员，另外组织商业秘密保护专题培训，包括但不限于：
- a) 对科研机构法定代表人、股东、高级管理人员开展商业秘密保护观念与管理策略培训；
  - b) 对科研机构从事商业秘密保护工作的专兼职人员开展商业秘密保护实务及技能培训；
  - c) 对科研机构涉密部门和涉密人员开展商业秘密泄密风险与保护义务培训；
  - d) 对科研机构商业秘密保护工作支持人员开展商业秘密保密工具与相关资源培训。
- 7.4 科研机构组织商业秘密宣传培训应有相应的计划文件、培训教程、实施程序及评价机制。
- 7.5 科研机构需保留商业秘密宣传培训的所有实施记录，包括但不限于：
- a) 实施日期、地点与实施方式；
  - b) 实施内容；
  - c) 实际参与的涉密部门；
  - d) 实际参与的涉密人员签到记录；
  - e) 实施成果记录，包括但不限于口头报告、文字报告、考核评价结果。
- 7.6 针对已实施的商业秘密宣传或培训，科研机构可定期进行涉密人员商业秘密保护意识或能力考核，同时保留考核记录，以利于进行奖惩及持续改进宣传与培训的内容。

## 8 商业秘密资产确认

### 8.1 实施要求

8.1.1 科研机构应定期进行商业秘密资产的识别与确认，包括但不限于：

- a) 确定商业秘密的权益基础；
- b) 确定商业秘密具体客观存在事实；
- c) 确定商业秘密保护重点与管理的范围；
- d) 确定商业秘密授权、转让、质押、融资、作价入股等合法交易的具体标的；
- e) 确定商业秘密鉴定或诉讼维权时的具体客观证据已获得保全固化。

注：将商业秘密视为资产来进行管理，其目的是确保科研组织能行使占有、使用、收益、处分的权利，进而获取经济利益等商业秘密权益基础，商业秘密资产与科技成果转化有直接的关系。

8.1.2 商业秘密资产确认的过程应包含商业秘密载体盘点、商业秘密载体归档与商业秘密电子存证。此过程主要适用于以电子档案为保存形式的商业秘密载体。

8.1.3 商业秘密资产确认的范围应采取最大化原则，以避免发生管理上的疏漏。

### 8.2 商业秘密载体盘点

8.2.1 科研机构应定期进行商业秘密载体盘点，切实掌握商业秘密载体动向。

8.2.2 科研机构应要求各涉密部门或专人落实商业秘密载体盘点。因商业秘密载体盘点需较强的专业性和知识产权背景知识，科研机构可与有相关资质的司法鉴定机构共同参与、实施商业秘密载体盘点。盘点前，司法鉴定机构应签订第三方保密协议。

8.2.3 科研机构应基于所属行业、部门组织或项目组织等不同情形，进行商业秘密载体的分类管理。

8.2.4 科研机构进行商业秘密载体盘点后，应以商业秘密载体清单或商业秘密盘点表等方式管理。

8.2.5 科研机构进行商业秘密载体盘点，应包含但不限于：

- a) 商业秘密载体盘点实施日期；

- b) 商业秘密载体盘点部门名称;
  - c) 商业秘密载体涉密信息类别, 如技术信息或经营信息;
  - d) 商业秘密载体业务或项目类别;
  - e) 商业秘密载体名称, 如电子档案名称、器材设备名称、原料物件名称;
  - f) 商业秘密载体形式, 如电子档案、实体图纸、原料物件、制造器具;
  - g) 商业秘密载体取得方式说明, 如自行研发、技术购入、并购取得;
  - h) 商业秘密载体保管部门及保管人员;
  - i) 其他有助于科研机构进行商业秘密载体保护的信息, 如保密分级、归档结果、存证结果。
- 8.2.6 下列可认定为公众所知悉的信息, 不应归属为科研机构保护的商业秘密资产, 不应列入商业秘密载体清单或商业秘密盘点表:
- a) 所属领域属于一般常识或者行业惯例的;
  - b) 所属领域的相关人员通过观察上市产品或实施反向工程即可直接获得的;
  - c) 已经在公开出版物或者其他媒体上公开披露的;
  - d) 已通过公开的研讨会议、展览等方式公开的;
  - e) 所属领域的相关人员从其他公开渠道可以获得该信息的;
  - f) 公知信息和基础理论;
  - g) 已申请并公开的专利;
  - h) 科研机构以其他方式公开的信息;
  - i) 可通过合法渠道获得的公开信息;
  - j) 法律法规规定的其他情形。
- 8.2.7 涉密部门主管应为该部门商业秘密载体盘点第一负责人, 保证商业秘密识别正确且完整地清查、记录与保存。
- 8.2.8 各涉密部门商业秘密载体盘点结果仅限该部门涉密人员知悉, 不应向其他部门揭露。
- 8.2.9 科研机构商业秘密管理组织应负责管控所有涉密部门商业秘密载体盘点结果, 负责监督与考核。
- ### 8.3 商业秘密载体归档
- 8.3.1 科研机构应制定明确的商业秘密载体归档相关实施办法, 内容应包括但不限于商业秘密载体归档的实施单位、档案格式、版本频率、审核方式、操作方式、登记内容。
- 8.3.2 商业秘密载体应由指定的档案保管部门负责集中保存与管理, 确保商业秘密载体的真实性、可靠性、完整性与可用性。
- 8.3.3 通过商业秘密资产盘点程序, 且认定为商业秘密载体的档案, 应列入归档保护的范畴。
- 8.3.4 商业秘密管理组织应根据各部门商业秘密资产盘点结果, 不定期进行查验、监督与考核, 确保商业秘密载体如实完成归档程序。
- 8.3.5 商业秘密载体正式归档前, 应由涉密部门负责核对档案的真实性、完整性和有效性。
- 8.3.6 档案保管部门收到涉密部门申请进行归档并完整移交商业秘密载体后, 应进行核对与登记。
- 8.3.7 档案保管部门应将指定归档的商业秘密载体存入专用的存储设备或系统中, 并进行封存。
- 8.3.8 科研机构应采用可长期保存、不易遗失且具有信息安全保护能力的存储设备保存商业秘密载体。
- 8.3.9 针对档案保管部门已封存的商业秘密载体, 不应调阅、编辑、移动、删除、变造、重制、毁损或遗失, 除非获得商业秘密管理组织授权许可。
- 8.3.10 商业秘密载体封存的期限应为永久保存或设定合理的解封期限。
- 8.3.11 档案保管部门应保有商业秘密载体归档及封存过程的申请、审核、登记与操作日志等记录。
- ### 8.4 商业秘密电子存证
- #### 8.4.1 评估阶段
- 8.4.1.1 科研机构进行商业秘密载体存证前, 应对所采用的电子数据存证平台进行以下审查:
- a) 存证平台是否符合国家有关部门关于提供区块链存证服务的相关规定;
  - b) 当事人与存证平台是否存在利害关系, 以及是否存在利用技术手段不当干预取证、存证过程的情况;

- c) 存证平台的信息系统是否符合 SF/T 0076—2020 的要求；
  - d) 存证技术和过程是否符合相关具体国家标准或者行业标准中关于系统环境、技术安全、加密方式、数据传输、信息验证等方面的要求；
  - e) 存证平台应达到 GB/T 22239—2019 的第三级基本要求并通过网络安全等级保护第三级测评。
- 8.4.1.2 电子数据存证平台宜引入外部参与者作为鉴证节点，强化存证效力，并对电子数据内容有效性作出独立判断。外部相关方包括但不限于公证处、仲裁机构、鉴定机构、授时服务机构、数字身份认证中心。

#### 8.4.2 准备阶段

- 8.4.2.1 科研机构应通过电子数据存证服务提供者对于服务使用方的实名身份核验并签署有效的服务协议。
- 8.4.2.2 科研机构应优先采用不需要原文存证的电子数据存证方式，仅提交通过电子数据存证服务提供者提供的哈希值算法得到的哈希值来取得存证证明。如科研机构需要进行原文存证的，应提交商业秘密存证原件到电子数据存证平台，且在提交前应仔细确认电子数据存证平台对于商业秘密存证原件的搜集、处理、利用与保管的方式，明确了解双方权利义务，事先评估风险，以避免产生纠纷。
- 8.4.2.3 科研机构应于每次正式进行商业秘密载体存证前，再次确认电子数据存证平台的真实性、可靠性、完整性与可用性。
- 8.4.2.4 科研机构应指派专人负责进行商业秘密载体存证，且确认该人员已具备电子数据存证平台的操作能力。

#### 8.4.3 实施阶段

- 8.4.3.1 科研机构应遵循依法正当、诚实信用原则，确保证明原件的真实性，不应伪造或篡改。
- 8.4.3.2 科研机构用来进行商业秘密电子存证的相关权利证明原件，包括但不限于：
- a) 已完成归档的商业秘密载体；
  - b) 商业秘密管理或保密制度文件；
  - c) 商业秘密管理或保护的实施记录；
  - d) 研发历程记录，如研发日志、技术会议记录、历程文件记录、研发费用支出等证明；
  - e) 业务历程记录，如客户往来通讯、议价交易记录、客户需求、业务费用支出等证明；
  - f) 法律文件签订记录，如保密协议、竞业限制协议、技术取得或授权协议等证明；
  - g) 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；
  - h) 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；
  - i) 泄密人员能够接触商业秘密的证据；
  - j) 商业秘密权利被侵犯的证据或受到损害的证据；
  - k) 其他有利于科研机构证明自主商业秘密权利与未侵害他方商业秘密权利的证据。
- 8.4.3.3 科研机构工作人员调取商业秘密存证原件进行存证前，应遵循相应的审核程序且保留记录。
- 8.4.3.4 科研机构进行商业秘密存证时，应提供有关必要的信息，包括但不限于：
- a) 商业秘密存证原件的档案名称、摘要说明、哈希值、权利人名称；
  - b) 商业秘密存证服务的申请人姓名；
  - c) 商业秘密存证的可信时间标识；
  - d) 其他有利于科研机构辨识与管理商业秘密存证原件的元数据。
- 8.4.3.5 科研机构完成存证后，应向电子数据存证服务提供者索要签发存证凭证。存证凭证包括但不限于以下的明文信息：
- a) 电子数据存证服务提供者或凭证核发单位名称；
  - b) 电子数据存证平台名称；
  - c) 存证凭证编号；
  - d) 商业秘密存证原件的权利人名称；
  - e) 商业秘密存证服务的申请人姓名；

- f) 商业秘密存证服务的可信时间标识;
- g) 商业秘密存证原件的哈希值;
- h) 可供科研机构或他方进行核验存证结果的信息;
- i) 其他外部参与者作为鉴证节点的信息。

8.4.3.6 如发现以下事件, 科研机构应重新进行存证, 以确保存证效力不受质疑:

- a) 前次存证操作未成功;
- b) 先前存证所使用商业秘密存证原件, 其内容发生变更、已有更新的内容版本、其申请数据信息内容需要更新、发生毁损或遗失等状况;
- c) 先前的存证凭证无法通过查验。

8.4.3.7 科研机构应完整保存每次电子数据存证的正本记录证据, 包括商业秘密存证原件、存证凭证、存证操作记录等, 且不应事后伪造或篡改。

#### 8.4.4 查验阶段

8.4.4.1 科研机构有取证或调证需求时, 应由科研机构商业秘密管理组织设置申请审核窗口, 指派专人进行查验。

8.4.4.2 科研机构向电子数据存证服务提供者申请查验存证记录, 如存证凭证的真伪、存证凭证的效力、完成存证的时间、存证原件的哈希值、区块链地址等信息。

### 9 商业秘密资产内部保护

#### 9.1 涉密岗位管理

科研机构应根据工作情况明确涉密岗位, 将涉密岗位划分为核心涉密岗位、重要涉密岗位和一般涉密岗位。在涉密岗位工作的人员应遵循涉密人员管理要求。

#### 9.2 涉密人员管理

##### 9.2.1 入职管理

对于新入职、到岗的涉密人员, 应采取以下管理措施:

- a) 新入职、到岗到涉密岗位的人员, 与其签订与岗位工作内容相适应的保密合同或协议, 明确约定保密义务以及违约责任等;
- b) 高级管理人员、高级技术人员及其他负有保密义务的重要涉密人员(如技术、采购、销售等有机会接触、利用重要或关键商业秘密的人员), 对因保密原因合法权益受到影响和限制的涉密人员, 按照国家有关规定给予相应待遇或者补偿, 可另与涉密人员签订竞业限制协议, 明确约定保密义务以及竞业限制的范围、地域、生效条件、期限、违约责任、经济补偿条件等;
- c) 对所有待录用涉密人员的背景进行验证核查, 核实其是否对前雇主负有保密义务或竞业限制义务, 且保留验证核查记录;
- d) 提醒待录用的涉密人员, 不将原任职机构的商业秘密带入本科研机构进行使用或公开, 并保留提醒的记录, 要求其签署不侵犯原任职机构商业秘密的承诺函。

##### 9.2.2 履职管理

对于在职的涉密人员, 应采取以下管理措施:

- a) 要求所有涉密人员熟悉并履行商业秘密管理制度及各项管理工作;
- b) 要求所有人员定期参与商业秘密保护的保密宣传及培训工作;
- c) 建立商业秘密管理奖惩制度, 鼓励工作人员积极创新研发, 上报有关商业秘密管理体系、保密策略、保密措施等的漏洞, 对科技创新成果带来显著贡献或发现并举报违反商业秘密管理规定的行为给予奖励, 对违反商业秘密管理规定的行为进行处罚;
- d) 根据涉密岗位及各部门接触商业秘密的情况, 建立涉密岗位及涉密人员清单;
- e) 督促岗位变动人员做好保密材料交接工作, 对人员重新划分涉密类别与层级, 及时做好涉密

接触权限的调整；

- f) 参加涉及商业秘密的工作会议等活动，采取相应的保密措施。

### 9.2.3 兼职管理

对于科研机构在外兼职的涉密人员，科研机构应采取以下管理措施：

- a) 根据涉密岗位及各部门实际接触商业秘密以及在外兼职等情况，建立兼职人员名册清单、在外兼职单位与参与外部项目清单；
- b) 与从事兼职活动的人员、兼职单位三方共同签署兼职协议，或与从事兼职活动的人员签署双方协议，以进一步明确各方保密义务以及知识产权权属或权利划分等约定；
- c) 留存兼职人员在兼职期间从事相关研发工作的基础资料、研发数据、设备等物资的使用记录等证据资料；
- d) 关注科研人员在外兼职单位近期的商业秘密侵害风险，对疑似涉入商业秘密或其他知识产权争议案件的单位，评估是否启动内部预警调查与列入警示名单。

### 9.2.4 离职管理

对于涉密人员离职，应采取以下管理措施：

- a) 涉密岗位人员离职前，主动面谈并告知其负有的保密义务，以及若违反规定应承担的相应法律责任。同时告知离职人员不应有以下行为：
  - 私自复制、带离、损毁、篡改、拍摄涉密文件资料、物品；
  - 私自查阅、拷贝、篡改、发送涉密电子文档、数据；
  - 私自删除、更改账户；
  - 私自披露、使用商业秘密；
  - 其他侵害商业秘密的行为。
- b) 要求待离职涉密人员主动移交一切涉密载体和物品，并进行盘点和登记；
- c) 对待离职涉密人员（尤其对重点涉密人员）做好离职审计。离职审计包括但不限于以下内容：
  - 待离职涉密人员所使用的电脑上是否有权限之外的文档；
  - 待离职涉密人员所使用的电脑数据是否完整，是否有异常删除或复制的痕迹；
  - 待离职涉密人员所使用的信息系统，包括数据库或邮件系统等，其访问日志是否有异常；
  - 涉密人员在申请离职前一定期限内的商业秘密的查阅和使用情况是否有异常。
- d) 主动探询待离职涉密人员该部门的相关人员，了解该人员离职原因是否涉及竞争对手就业或其他可能涉及泄密窃密的风险因素；
- e) 在离职审计过程中，若发现涉密人员可能存在侵害商业秘密行为的，应及时收集并固定证据，按照泄密事件管理的规定处理；
- f) 对待离职涉密人员采取适当措施进行脱密，及时回收系统权限，并及时通知与离职人员有关的外部供应商、客户、合作单位等，做好业务交接；
- g) 采取适当的方式或约定内容，进行离职人员追踪，并掌握已签订竞业限制协议的离职人员于竞业限制期限内的任职去向。

### 9.2.5 外部人员来访管理

对于外部来访人员，应采取以下管理措施：

- a) 外部来访人员进入科研机构涉密区域经审批，履行进出登记，且全程佩戴临时证件；
- b) 外部来访人员进入涉密区域，受访部门安排人员陪同，限制来访人员使用具有录音、摄像、拍照、信息存储等功能的设备；
- c) 外部来访人员进入涉密区域，限制其使用网络接收、处理与传输信息的能力；
- d) 科研机构与外部人员召开重要涉密会议，主动告知相关保密义务并采取适当的保密措施；
- e) 外部人员如需使用或外出携带商业秘密载体，包括但不限于电子档案、实体物品，由受访部门事先核实外部人员及其所任职的单位是否已签订相应的有效保密协议，同时依据科研机构商业秘密管理制度的相关要求实施保密措施，并保留外部人员每次接触、使用或外出携带商

业秘密载体的签署记录；

- f) 政府职能部门及其工作人员、第三方专业机构、专家、观察员等对参与调查过程中知悉的商业秘密负有保密义务。

### 9.3 涉密文档管理

#### 9.3.1 分级标示

对于涉密文档，应采取分级标示措施：

- 科研机构根据商业秘密泄露后可能对自身生存发展和利益造成的损害程度进行评估，将商业秘密载体进行分级管理，商业秘密载体分级见表 1；
- 商业秘密载体标记相应的提示警语文字与密级标识，任何人不私自删除、涂改或遮蔽商业秘密文件的密级标识；
- 科研机构严格要求工作人员落实分级与标示，且不定期进行抽查及考核。

表 1 商业秘密载体分级方式

商业秘密载体分级	含义解释
秘密	指一般的商业秘密，泄露会使科研机构生存发展和利益遭受损害
机密	指重要的商业秘密，泄露会使科研机构生存发展和利益遭受严重的损害
绝密	指最重要的商业秘密，泄露会使科研机构生存发展和利益遭受特别严重的损害

#### 9.3.2 储存保管

对于涉密文档储存保管，应采取以下管理措施：

- 各涉密部门指定专人负责该部门的商业秘密载体存档和保管工作；
- 科研机构定期对商业秘密载体进行备份；
- 商业秘密载体存放在科研机构监管下的实体储存处或指定的信息系统，避免在办公电脑、信息系统和设备以外的任何装置进行存储，如有特殊或例外情况需在科研机构规定范围外的装置存储商业秘密载体，事先提交相关申请，且获得涉密部门主管审批同意；
- 实体形式的商业秘密载体保存方式与其他一般文件或物品有所区隔，或使用上锁的储物柜，指定专人保管，且定期根据商业秘密载体清单或商业秘密盘点表进行核对；
- 科研机构存放商业秘密载体的区域配备监控摄像头、火灾报警等安防设备。

#### 9.3.3 内部流通

对于涉密文档内部流通，应采取以下管理措施：

- 规定与限制人员使用商业秘密载体的场地、时机、条件、设备与方式；
- 规定人员在进行商业秘密载体的复制（拷贝、打印、扫描、摘抄等）、跨部门或项目转移、披露或使用之前，由涉密部门主管审批并完成登记手续，复制件与原件的密级相同；
- 规定人员取得或提供商业秘密载体的传输方式，包括但不限于指定的网络环境、邮件系统、储存系统、收发件流程或密封包（箱）；
- 商业秘密载体的请求与交付过程，基于“仅需要知道的原则”（Need To Know Basis）审慎处理，凡超过涉密部门业务范围、项目范围、职务范围之外，无需过度知悉的商业秘密信息，不进行接触或流通；
- 制定标准化的档案命名与版本编号等原则，易于快速辨识与遵守实施；
- 科研机构对于人员实际接触商业秘密载体或密点信息的行为保有操作日志或相关记录。

#### 9.3.4 加密保护

对于涉密文档加密保护，采取以下管理措施：

- a) 宜采用加密系统强化商业秘密载体的保护能力，加密系统应采取密钥备份、双人控制以及意外恢复还原等安全管理措施；
- b) 宜制定档案加密及解密的规范或程序，包含但不限于操作对象、操作时机、审批机制、应急预案。

### 9.3.5 删除销毁

对于涉密文档删除销毁，应采取以下管理措施：

- a) 所有人员不随意弃置、丢弃或毁损商业秘密信息载体；
- b) 销毁涉及商业秘密的文件、资料、电子信息、载体和物品，由涉密部门专责人员列出销毁清单与事由，经商业秘密管理组织审批后实施；
- c) 商业秘密信息载体的销毁过程采取监督措施，如视频监控、录像、见证；
- d) 根据商业秘密信息载体的不同采取妥善的销毁方式，确保信息不可恢复。

### 9.3.6 留痕记录

对于涉密文档留痕记录，应采取以下管理措施：

- a) 所有商业秘密载体在科研机构内部的产生、分级、保存、流通、加解密及销毁等保留记录；
- b) 留痕记录的保存时间与方式由商业秘密管理组织进行评估与核定。

## 9.4 涉密系统管理

### 9.4.1 账号密码

对于涉密系统账号密码管理，应采取以下管理措施：

- a) 视业务或任务需求，为工作人员设置可登录办公电脑设备、数据库、档案库或应用系统的账户和密码；
- b) 账号和密码属于个别人员且仅限本人保管使用，不与其他人员共用；
- c) 避免使用默认密码或保存密码等方式自动登录信息系统；
- d) 制定密码强度（长度）规则；
- e) 信息系统的密码通过系统设置强制用户定期更换；
- f) 业务部门设置公用账号、匿名账号等特殊账号，经过商业秘密管理组织审批；
- g) 信息系统的账号密码建立申请、登记、审核、发放及撤销等作业办法，由专人负责管理并保留所有变更记录。

### 9.4.2 权限管理

对于涉密系统权限管理，应采取以下管理措施：

- a) 由商业秘密管理组织统一管理对涉密信息系统的授权使用范围与条件；
- b) 由商业秘密管理组织制定涉密信息系统账号权限的申请或变更审批办法；
- c) 对接触商业秘密信息的相关涉密系统的人员，如办公电脑设备、数据库和各类应用系统，为其账户实行权限管理，以“最小够用”原则设定权限；
- d) 涉密系统的权限至少包括可使用系统的期限、可操作的功能范围、可操作的数据或档案范围等；
- e) 权限到期、人员变更、转岗或离职、项目变更时，及时变更、撤销相应的信息系统权限；
- f) 信息系统的权限变更事件保留完整记录日志；
- g) 信息系统的管理员权限在不同人员之间进行分配，避免由超级管理员管理整个系统或多个系统的情况。

### 9.4.3 办公电脑

对于涉密系统办公电脑，应采取以下管理措施：

- a) 科研机构配备办公电脑供工作人员公务使用，且作为主要的商业秘密信息处理设备；
- b) 工作人员携带个人电脑至科研机构办公，由商业秘密管理组织审批核定，科研机构可视人员

职务涉密程度与权限层级，要求限制其个人电脑的信息处理能力，包括但不限于不在本地端储存商业秘密载体、不接入特定科研机构内部网络、需同意安装电脑行为监控软件；

- c) 关闭或禁用办公电脑的移动存储等数据传输功能模块，以及音视频采集设备，未经许可不得使用；
- d) 办公电脑硬件的配置、维修、报废均经过审批或授权交由指定人员处理，使用封条封住主机以禁止工作人员私自拆机维修、更换、增加硬件配件；
- e) 办公电脑未经批准不安装非授权软件；
- f) 办公电脑的网络接入、网络配置均按规定设置，禁止接入非授权网络；
- g) 可于办公电脑安装电脑行为监控软件，及早针对风险事件做出预警措施；
- h) 可于办公电脑安装杀毒或系统还原软件，降低系统因故损坏的风险。

#### 9.4.4 数据系统

对于涉密数据系统，应采取以下管理措施：

- a) 商业秘密载体存储于科研机构授权的数据系统，不存储于非授权的存储设备或网络空间；
- b) 工作人员使用科研机构核发的账号与密码才能进入并使用数据系统；
- c) 工作人员操作数据系统时，以下行为履行审批手续，非工作需要不得擅自使用或操作：
  - 需要超出权限查阅或使用商业秘密载体数据；
  - 需要拷贝或打印存储设备或应用系统中的商业秘密载体数据；
  - 需要上传、汇总商业秘密载体数据至第三方系统平台；
  - 需要变更或删除商业秘密载体数据。
- d) 科研机构保存工作人员使用数据系统的操作记录；
- e) 数据系统建立在科研机构完全可控的环境之中，易于系统管理、更新与维护；
- f) 数据系统有相应的信息安全保护机制，如防火墙、杀毒软件等；
- g) 数据系统定期进行备份以及信息安全漏洞检测；
- h) 数据系统有相应的灾害应变与系统复原措施。

#### 9.4.5 智能手机

对于涉密智能手机，应采取以下管理措施：

- a) 评估实际需求，列册核发专用的智能手机，供工作人员执行业务使用；
- b) 科研机构核发的智能手机由专人专管专用，且事先安装具有身份识别、内容加密、设备绑定、行为监控等保密措施的软件；
- c) 个人智能手机不接入存有科研机构商业秘密载体数据的系统，避免在个人手机内存储商业秘密信息；
- d) 涉密区域不使用个人智能手机，如携带个人智能手机进入涉密区域关闭或禁用摄像头、麦克风，不在涉密区域内拍摄、录音、设置热点；
- e) 个人智能手机不接入科研机构涉密网络。

#### 9.4.6 移动存储

对于涉密移动存储，应采取以下管理措施：

- a) 科研机构评估实际需求，列册核发专用的涉密移动存储设备，供工作人员执行业务使用；
- b) 涉密移动存储设备由专人专管专用，且使用具有身份识别、内容加密、设备绑定、行为监控等保密功能的设备；
- c) 工作人员完成任务后缴回涉密移动存储设备且确实清空存储内容；
- d) 未经审批不使用移动存储设备存储商业秘密载体，涉密移动存储介质不连接非涉密或未采取保密措施的计算机及电子设备；
- e) 未经审批不携带涉密移动存储设备至科研机构外部使用。

#### 9.4.7 信息传输



对于涉密信息传输，应采取以下管理措施：

- a) 限制工作人员进行商业秘密载体传输或交换的渠道，包括但不限于：
  - 科研机构专用的网盘；
  - 科研机构专用的邮箱；
  - 科研机构专用的即时通讯软件；
  - 科研机构专用的数据系统；
  - 科研机构专用的网络环境。
- b) 工作人员透过邮件或即时通讯软件进行商业秘密载体传输或交换时，于信息内文加注提示警告文字与密级标识，必要时得以加密方式进行档案传输；
- c) 工作人员收到疑似未经授权或许可的商业秘密载体或涉密信息时，主动通报业务部门主管或商业秘密管理组织，不进一步接触或使用该涉密档案；
- d) 科研机构的办公网络不允许工作人员访问非科研机构邮箱的外部邮箱，将常见的外部邮箱、地址包括网址设为禁止访问名单，因工作需要登录外部邮箱的经过审批并备案邮箱账号和密码；
- e) 禁止工作人员使用私人网盘，将常见的网盘网址设为禁止访问名单，确因工作需要登录私人网盘的经过审批，并向科研机构备案网盘账号和密码；
- f) 科研机构办公电脑使用的即时通讯软件避免和其他外部通讯软件交互商业秘密信息；
- g) 对于涉密信息的传输，科研机构具备权限管理、操作记录日志与行为监控等保密能力。

## 9.5 涉密区域管理

9.5.1 科研机构内部的办公区域应根据科研单位或项目的敏感程度、商业秘密信息储存与流通的密集程度，划分为不同等级的涉密区域。不同等级的区域之间应采取物理门、墙、隔断等物理隔离措施。涉密等级较高的办公区域应设置在离科研机构出入口相对较远的位置。

9.5.2 涉密区域可采取下列保密措施：

- a) 宜使用独立、封闭的办公区域，不宜使用开放式办公或多部门混合办公；
- b) 工作人员进出宜佩戴明显的身份标识卡，非授权人员因工作而出入涉密区域，需经审批取得临时授权；
- c) 涉密区域出入口应张贴“涉密级别”“禁止携带违禁品”或“禁止录音摄像”等警句标识；
- d) 宜配备安保人员及安防设备，安保人员需定时或不定时巡逻检查；
- e) 宜限制工作人员在较高等级涉密区域内使用个人信息设备或网络通讯的能力；
- f) 宜于涉密区域设置如面部或指纹等具有个人生物特征识别能力的安防系统；
- g) 有专人定期进行安全检查，清查任何可能造成泄密的不明装置或漏洞风险；
- h) 涉密区域内部可设置专门的涉密会议室或防窃听通讯装置；
- i) 涉密电脑屏幕可配备防偷窥、防拍照措施；
- j) 较高等级的涉密区域可评估是否适时关闭或遮蔽对外窗户，以避免外部窥视；
- k) 宜配备视频监控及报警系统，能对非法闯入或携带违禁品进入实时报警；
- l) 非经审批同意，不得擅自移动或携出涉密区域内的物品或设备，若获准携出涉密区域内的物品或设备，保留携出登记记录。

9.5.3 储存或备份商业秘密载体的数据中心、文档中心应设置在相对隐蔽的位置，远离非涉密区域且不宜张贴明确标识以防侵入。

9.5.4 科研机构可根据业务和保密要求的不同，将内部网络划分为不同的网络区域。涉密区域的涉密网络可采取以下保密措施：

- a) 禁止电脑或任何信息装置接入外网，或以白名单方式限制接入外网的能力；
- b) 与其他内部网络进行隔离，不能相互连通；
- c) 与其他内部网络采取不同的分级或权限管理措施；
- d) 禁止使用无线网络、无线热点；
- e) 访问涉密区域网络的设备使用终端准入限制、身份安全等验证措施；
- f) 配备独立的网络基础设施如服务器、防火墙、专线等。

9.5.5 科研机构应根据业务和保密等级要求，将较高等级的涉密区域设置在具有较高防灾能力的建筑中。

9.5.6 科研机构对外开放租借或共享研究设备、器材或场所（以下简称“共享平台”），可采取下列保密措施：

- a) 科研机构制定共享平台物理环境管理规范及使用规定；
- b) 共享平台设置专职管理员，负责共享平台的日常管理工作，包括但不限于共享设备的登记备案、使用时段预约与实际使用签到管理，并在每台设备上张贴标签以便于管理，标签内容包括设备责任人和紧急联系电话；
- c) 科研机构与外部申请方签订共享平台使用合同，严格要求按照操作流程进行实验研究；
- d) 共享平台所有设备与物理环境与科研机构涉密区域进行隔离，外部使用人员不接入可能接触科研机构商业秘密信息的内部网络、电脑或数据库等系统；
- e) 外部使用人员每次使用共享平台后，自行保存实验研究成果，每次使用结束后，由专职管理员进行设备检查并进行清空还原；
- f) 专职管理员定期进行共享平台安全检查，清查任何可能造成泄密的不明装置或漏洞风险。

## 10 商业秘密资产外部保护

### 10.1 信息公开

10.1.1 科研机构对外发布公开信息，发布人应注意识别和防范商业秘密泄露。对外发布公开信息包括但不限于：

- a) 学术论文；
- b) 专利文件；
- c) 产品说明文件；
- d) 技术成果展示；
- e) 依法需公开披露的组织运营报告；
- f) 科研机构自主发布的媒体新闻；
- g) 科研机构自主或受委托发布的调研报告书；
- h) 研讨会议或展会活动所揭露的信息。

10.1.2 商业秘密管理组织应建立科研机构信息公开时可能涉及商业秘密信息的保密审查制度。

10.1.3 科研机构正式对外发布公开信息时，应就可能涉及商业秘密的信息，进行遮挡或隐蔽。

### 10.2 商务活动

10.2.1 在开始商务谈判前或提供涉密信息前，应评估泄密风险，且与对方签署保密协议。

10.2.2 在商务谈判或提供涉密信息的过程中，应明确告知收受方对于取得涉密信息后的保密义务、使用范围及使用限制，妥善保存交付过程的签收证据。

10.2.3 在商务谈判或提供涉密信息内容之后，应监督追踪保密协议是否有效履行与相关涉密信息流向。

10.2.4 在商务活动中应避免泄漏科研机构重大政策方向、关键技术走向、产品研发计划、核心原料或零组件取得方式、涉密部门或涉密人员名单等可能让外部方恶意探查商业秘密来源途径的敏感信息。

### 10.3 委外服务

科研机构在正式聘任或委托外部专家、顾问、翻译、律师、会计师或技术供应厂商进行服务之前，宜进行背景调查，评估窃密或泄密风险，并应签订保密协议及不侵犯他方商业秘密承诺书。

### 10.4 科技成果转化

10.4.1 科研机构进行科技成果转化，应依法签订合同，明确各方享有的权益和各自承担的责任，并在合同中约定在科技成果转化过程中产生的后续改进技术成果的权属，包括商业秘密权属。科技成果转化包括但不限于：

- a) 自行投资实施转化；
- b) 向他人转让该科技成果；
- c) 有偿许可他人使用该科技成果；
- d) 以该科技成果为合作条件与他人共同实施转化；
- e) 以该科技成果作价投资折算股份或出资比例；
- f) 其他协商确定的合法方式。

10.4.2 科研机构应依照科技成果转化合同约定的内容、时间与方式，交付与该项科技成果相关的商业秘密涉密文件，且交付过程应保有完整的记录。

10.4.3 科技成果转化过程中涉及商业秘密转化或交付的，科研机构应与转化方签署相应的保密协议，保密协议应明确保密范围、保密期限、泄密补救措施、违约责任等内容。保密协议的法律效力独立于科技成果转化合同，不受科技成果转化合同效力影响。

## 11 检查与改进

11.1 商业秘密管理组织应要求涉密部门定期以书面方式报告商业秘密管理实施成果，确保科研机构商业秘密资产均在受控的保护范围内，并且有效运行。

11.2 商业秘密管理组织应定期举行检查与评审会议，针对定期评估报告发现的管理缺失、风险漏洞及不足的资源，制定调整方案及改进计划。

11.3 商业秘密管理组织应基于监督检查结果，落实完善商业秘密保护的奖惩机制。

11.4 商业秘密管理组织发现有泄密情况及隐患的，应及时采取纠正或预防措施。

11.5 商业秘密管理组织可适时采用外部第三方机构的认证机制，客观衡量科研机构商业秘密管理制度的保护效力与实施绩效。

11.6 商业秘密管理组织应留存商业秘密管理制度相关检查与改进的实施记录。

## 12 应急与维权

### 12.1 应急处置预案

科研机构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。应急处置预案应包括但不限于以下内容：

- a) 采取保护措施防止信息进一步扩散或损失扩大；
- b) 调查原因、涉事人员、责任人等；
- c) 收集并固定证据；
- d) 启动内部处罚或外部维权；
- e) 形成报告和改进方案；
- f) 涉及国家秘密的，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。

### 12.2 证据收集与固定

12.2.1 科研机构在获得行政主管部门、司法机关或商业秘密保护服务机构等机构或单位帮助和指导之前，发现商业秘密被侵犯时，应及时对以下证据进行收集、固定以便维权：

- a) 能够证明被侵权信息属于权利人主张的商业秘密的证据，包括科研机构已采取的保密措施、该信息的商业价值及非公知性；
- b) 商业秘密与侵权人掌握信息的实质性重合的证据；
- c) 能够证明侵权人通过不正当手段获取该信息的证据，或者在信息实质性相似的基础上能够证明对方接触该商业秘密的间接证据链；
- d) 商业秘密被侵权后的损失及与侵权行为间因果关系的证据；
- e) 科研机构在合作开发、委托加工等活动中，保留相关合同、协议，以便在相关方侵犯第三方商业秘密时，提供必要证据维护自身权益。

12.2.2 对于科研机构自主研发、合法受让或被许可、通过反向工程破解以及善意取得的商业秘密，应当保留相关证据以规避被恶意诉讼的损失。其中，涉及商业秘密的非公知性、同一性、损害赔偿额等证明时，可寻求第三方服务机构提供科技查新、鉴定评估等专业服务。

### 12.3 维权途径选择

科研机构商业秘密被侵犯，可视不同情况，采取不同维权途径：

- a) 寻求协商调解：科研机构与侵权人双方本着真实自愿的原则协商或委托共同认可的第三方进行调解；
- b) 寻求行政保护：科研机构的商业秘密被他人的不正当竞争行为侵犯，可以向有管辖权的商业秘密行政管理部门举报；
- c) 寻求民事保护：可依据有关法律法规，向仲裁机构申请仲裁，或者向法院提起民事诉讼，要求侵权人停止侵权并赔偿损失；
- d) 寻求刑事保护：侵犯商业秘密，造成商业秘密权利人损失数额在三十万元以上的，或者侵权人因侵犯商业秘密违法所得数额在三十万元以上的，或者致使商业秘密权利人破产的，或者致使商业秘密权利人遭受其他重大损失的，为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，商业秘密权利人可以向公安机关举报，追究侵权人的刑事责任。

## 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] GB/T 29490—2023 企业知识产权合规管理体系 要求
- [3] GB/T 33250—2016 科研组织知识产权管理规范
- [4] GB/T 37043—2018 智慧城市 术语
- [5] GB/T 43803—2024 科研机构评估指南
- [6] DB33/T 2273—2020 商业秘密保护管理与服务规范
- [7] DB43/T 2652—2023 企业商业秘密保护管理规范
- [8] DB4403/T 235—2022 企业商业秘密管理规范
- [9] T/CESA 1048—2018 区块链存证应用指南
- [10] T/PPAC 701—2021 企业商业秘密管理规范
- [11] T/SHSFJD 0001—2020 基于区块链技术的电子数据存证规范
- [12] 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（2019年修正）：中华人民共和国主席令第29号. 2019年
- [13] 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
- [14] 中华人民共和国全国人民代表大会常务委员会. 中华人民共和国刑法修正案（十一）：中华人民共和国主席令第66号. 2022年
- [15] 中华人民共和国全国人民代表大会常务委员会. 《中华人民共和国保守国家秘密法》，中华人民共和国主席令第20号. 2024年
- [16] 最高人民法院. 《最高人民法院关于互联网法院审理案件若干问题的规定》：法释〔2018〕16号. 2018年
- [17] 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
- [18] 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
- [19] 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具体应用法律若干问题的解释》：法释〔2004〕19号. 2020年
- [20] 最高人民法院. 《人民法院在线诉讼规则》：法释〔2021〕12号. 2021年
- [21] 国家市场监督管理总局. 《网络反不正当竞争暂行规定》：总局令91号. 2024年
- [22] 江苏省高级人民法院. 《江苏省高级人民法院侵犯商业秘密民事纠纷案件审理指南（2021年修订）》：江苏省高级人民法院审判委员会会议纪要〔2021〕2号. 2021年
- [23] 北京知识产权法院. 《北京知识产权法院侵犯商业秘密民事案件诉讼举证参考》. 2021年
- [24] 上海技术交易所. 《上海技术交易所企业商业秘密资产确权管理指引》. 2022年
- [25] 深圳市人民检察院. 《商业秘密刑事保护体系合规建设指引（试行）》. 2023年