

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、科研院所等。

[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的，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围。
- 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，确保存证原件的真实性，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；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/716235015200010221>