ICS 03.140
CCS A 10

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXX—XXXX

科研机构商业秘密保护管理规范

Specification for the protection and management of trade secrets in scientific research institutions

（送审稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

深圳市市场监督管理局　　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》给出的规则起草。

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光明监管局、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。

本文件主要起草人：陈建民、吴良卫、李飞、李富山、梁光宇、吴毅勋、刘莹莹、张智禹、朱谢群、邓映均、谭丽、王磊。

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、商业秘密管理组织、管理制度、宣传培训、资产确认、资产内部保护、资产外部保护、检查与改进的要求。

本文件主要适用于深圳市各类科研机构在研发、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。

2 规范性引用文件

本文件没有规范性引用文件。

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 scientific research institutions

是指有明确的任务和研究方向，有一定学术水平的业务骨干和一定数量的研究人员，具有开展研究、开发等学术工作的基本条件，主要进行科学研究与技术开发活动，并且在行政上有独立的组织形式，财务上独立核算盈亏，有权与其他单位签订合同，在银行有独立账户的独立法人。

3.2

商业秘密 trade secrets

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。

3.3

技术信息 technical information

是指与技术有关的结构、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。

3.4

经营信息 business information

是指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。

3.5

密点 secret points

是指权利人请求保护，区别于公众所知悉的技术信息、经营信息等商业信息的核心信息部分。密点用来体现权利人商业秘密保护的权利边界和范围，是商业秘密维权的基础，是权利人据以主张权利的依据。

3.6

商业秘密载体 secret-related carriers

是指承载有商业秘密密点内容的物品、设备或产品。

商业秘密载体包括但不仅限于以文字、数据、符号、实物、图形、图像、视频和音频等形式记载和存储商业秘密的电子档案、信息系统、纸本文件、制造物料、实验样本、器械工具、物理环境等，以及通过观察或者测试、分析手段能够获得商业秘密的设备或产品。

3.7

涉密人员 secret-related personnel

是指在工作中能够产出、接触、使用、掌握商业秘密的科研机构员工。

3.8

涉密部门 secret-involved department

是指在工作中能够产出、接触、使用、掌握商业秘密的科研机构内部单位。

3.9

涉密区域 secret-related places

是指存有商业秘密载体，人员进入后能够接触到商业秘密的物理区域，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。

3.10

元数据 metadata

是指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。

3.11

归档 file/ archive

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

3.12

备份 backups

是指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。

3.13

封存 seal up for safekeeping

是指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。

3.14

电子数据存证 electronic data storage certificate

是指通过互联网向科研机构提供电子数据证据保管和验证的服务。

3.15

电子数据存证服务提供者 electronic data certification service provider

是指提供电子数据存证服务的机构或组织。

3.16

电子数据存证平台 electronic data certification platform

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

3.17

可信时间戳 trusted trusted timestamp

是指唯一的标识某一刻时间的字符序列。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。

3.18

区块链 blockchain

是指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。

3.19

哈希值 hash value

又称杂凑函数或杂凑算法，是指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。哈希值通常用一个短的随机字母和数字组成的字符串来代表，因具有密码学上的不可逆性，故在电子数据取证领域常用作校验数据的完整性。

3.20

商业秘密存证原件 original copy of trade secret certificate

是指科研机构实际提交至电子数据存证平台，用以实际进行存证的原始档案。

3.21

存证凭证 certificate of deposit

是指由电子数据存证服务提供者核发，可作为存证保全结果的证明文件。

3.22

商业秘密资产 trade secret assets

是指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、依法维权”的商业秘密保护和管理原则。

4.2 科研机构应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的全部经营活动中，包括但不限于生产、研发、销售、采购、财务、人事、行政、商业合作等，并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，且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。

4.4 科研机构应主动积极建立合法与合规的管理文化，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。

5 商业秘密管理组织

5.1 科研机构最高管理者应具备正确的商业秘密管理意识，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，让商业秘密管理体系可以稳健运行；
c) 将商业秘密管理要求整合到科研机构的业务流程中；

d） 要求员工建立并加强商业秘密保护意识；
e） 管理并支持员工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利。

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，各业务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。主要任务包括但不限于以下事项：

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） 确定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，听取商业秘密管理工作汇报并提出工作要求或计划，促进
g） 商业秘密管理体系的持续改进；
h） 指导、抽查和监督商业秘密管理工作的贯彻落实情况；
i） 对各部门的商业秘密管理工作进行评核、表彰和奖惩；
j） 指导开展商业秘密管理的宣传与培训工作；
k） 积极争取政府或其他外部单位的协同支持；
l） 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员工，具体开展商业秘密管理工作。主要任务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） 协助其他员工建立正确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） 即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 科研机构建立商业秘密管理组织应有相应的计划文件、规范文件、程序文件及管理表单。

6 商业秘密管理制度

6.1 科研机构应制定适用于本单位的商业秘密管理制度文件，包括但不限于以下内容：

a） 商业秘密管理的目的、目标、方针、适用范围、定义、策略、原则等；
b） 商业秘密管理的组织架构、职责与分工、年度工作计划等；
c） 商业秘密管理的培训实施方式；
d） 涉密人员的管理方式，包括责任与奖惩方式；
e） 涉密部门的管理方式；
f） 商业秘密资产载体的管理方式；
g） 专利与商业秘密协同管理的方式；
h） 核心供应商的管理方式；
i） 客户专项的管理方式；
j） 涉密系统的管理方式；

k） 涉密区域的管理方式；
l） 商业秘密管理的监督考核机制；
m） 商业秘密泄密应急处理机制。

6.2 科研机构的商业秘密管理制度应由商业秘密管理领导部门负责指导、编制、核定及发布。

6.3 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，并在组织内部进行正式公示与发布。

6.4 科研机构的商业秘密管理制度应有相应的管理文件、程序措施及管理表单。

6.5 科研机构应每年定期检查、修订与优化商业秘密管理制度，确保制度持续适用可用。

7 商业秘密宣传培训

7.1 科研机构应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以下内容：

a） 发放员工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等。

7.2 科研机构应对所有员工开展商业秘密保护与保密培训，以确保员工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：

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） 如何辨识与合法使用科研机构的商业秘密资产；
d） 哪些行为可能泄露或侵害科研机构的商业秘密；
e） 侵害商业秘密可能承担的法律责任；
f） 商业秘密司法判决案例；
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、职务或权限的员工，另外组织商业秘密保护专题培训，包括但不限于以下内容：

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） 对科研机构商业秘密保护重点岗位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 科研机构应保留商业秘密宣传培训的所有实施记录，包括但不限于以下内容：

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员工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 实施方针

8.1.1 科研机构应定期进行商业秘密资产的识别与确认。其实施目的包括但不限于：

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

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。

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，应包含但不限于以下内容：

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、原料物件名称等；
f） 商业秘密载体形式，如电子档案、实体图纸、原料物件、制造器具等；
g） 商业秘密载体取得方式说明，例如自行研发、技术购入、并购取得等；
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，如密点分级、归档结果、存证结果等。

8.2.6 下列可认定为公众所知悉的信息，不归属为科研机构保护的商业秘密资产，不得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的清查、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。

8.2.10 科研机构实施商业秘密载体盘点应有相应的计划文件、规范文件、程序文件及管理表单。

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：

a） 商业秘密载体归档的实施单位；
b） 商业秘密载体归档的档案格式；
c） 商业秘密载体归档的版本频率；
d） 商业秘密载体归档的审核方式；

e） 商业秘密载体归档的操作方式；
f） 商业秘密载体归档的登记内容。

8.3.2 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 凡是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，均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，除非获得商业秘密管理组织授权许可，否则不得调阅、不得编辑、不得移动、不得删除、不得变造、不得重制、不得毁损与不得遗失。

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 科研机构实施商业秘密载体归档应有相应的计划文件、规范文件、程序文件及管理表单。

8.3.12 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，并利用技术手段不当干预取证、存证过程；
c） 存证平台的信息系统是否符合清洁性、安全性、可靠性、可用性的国家标准或者行业标准；
d） 存证技术和过程是否符合相关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、
e） 数据传输、信息验证等方面的要求。

8.4.1.2 科研机构进行商业秘密载体存证前，所采用的电子数据存证平台应具有以下技术条件。
a） 电子数据存证平台的系统或软件可全时间稳定运行；
b） 电子数据存证平台存证数据所使用的物理设备及环境有完善的监控体系；
c） 电子数据存证服务提供者已采取措施保障电子数据存证平台安全，预防非授权的访问或破坏；
d） 电子数据存证服务提供者对于非授权的访问或破坏有防护措施和应急预案；
e） 电子数据存证平台具备冗余备份和存储扩展的能力，并具备异地容灾能力；
f） 电子数据存证平台有定期进行检查，防止网络攻击、病毒和网络代理的使用；
g） 电子数据存证平台已采用符合国家密码管理主管部门认证核准的密码技术对数据进行加密传
h） 输和存储，并对密钥采取必要的保护机制；
i） 电子数据存证服务提供者可保证电子数据存储和传输过程涉及的系统和软件完全可控，系统
j） 接口及系统配置安全可靠，避免系统代码被反编译或篡改。

8.4.1.3 电子数据存证平台应采用符合国际和国家标准认可的技术，采用的技术包括但不限于：
a） 可信计算技术；
b） 校验技术；
c） 数字签名技术；
d） 电子身份认证技术；
e） 可信时间戳技术；
f） 区块链技术；
g） 加解密技术；
h） 智能合约技术；
i） 分布式存储和计算技术；
j） 云计算和大数据技术；
k） 存储虚拟化技术。

8.4.1.4 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，且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：

a) 司法机关：是行使司法权的国家机关，是国家机构的基本组成部分，是为了保证法律实施而
b) 建立的相关组织；
c) 公证处：依法独立行使公证职能、承担民事责任的证明机构；
d) 仲裁机构：通过仲裁方式解决民事争议，作出仲裁裁决的机构；
e) 司法鉴定中心：利用科学技术或专门司法知识为司法相关问题提供鉴定意见的机构；
f) 授时服务机构：承担标准时间的产生、保持与发播，提供标准时间授时服务的机构；
g) 数字身份认证中心：提供数字证书的颁发、核验服务的机构。

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，仅通过提交可代表商业秘密存证原件唯一识别值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，且确认该员工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，不得伪造或篡改。

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，应包括但不限于：

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，例如研发日志、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，例如客户往来通讯、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，例如保密协议、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
i) 行价值评估；
j) 泄密人员能够接触商业秘密的证据；
k) 商业秘密权利被侵犯的证据或受到损害的证据；
l) 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 员工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，应提供包括但不限于以下必要的数据信息：

a) 商业秘密存证原件的档案名称；
b) 商业秘密存证原件的摘要说明；
c) 商业秘密存证原件的哈希值 ；
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) 商业秘密存证的可信时间戳标识 ；
g) 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 科研机构每次完成存证后，均应向电子数据存证服务提供者要求签发存证凭证。存证凭证应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戳（或时间标识）；
g） 商业秘密存证原件的哈希值编码；
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；
c） 先前存证所使用商业秘密存证原件，已有更新的内容版本；
d） 先前存证所使用商业秘密存证原件，其申请数据信息内容需要更新；
e） 先前存证所使用商业秘密存证原件，发生毁损或遗失等状况；
f） 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，且不得事后伪造或篡改。包括：
a） 商业秘密存证原件；
b） 商业秘密存证凭证；
c） 商业秘密存证操作记录。

8.4.4 查验阶段

8.4.4.1 如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 科研机构应向电子数据存证服务提供者申请查验存证记录，包括但不限于存证凭证的真伪、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。为司法、行政等部门依法准确查明事实，提供直接可信的证据。

8.4.5 科研机构实施商业秘密电子存证应有相应的计划文件、规范文件、程序文件及管理表单。

9 商业秘密资产内部保护

9.1 涉密人员管理

9.1.1 员工入职管理

对于新入职、到岗的人员，应采取以下管理措施：
a） 新入职、转岗到涉密岗位的员工，应与其签订与岗位工作内容相适应的员工保密合同或协议，
b） 明确约定保密义务以及违约责任等；
c） 高级管理人员、高级技术人员及其他负有保密义务的涉密人员（如科学家、高级工程师、院
d） 长、所长、主任、技术、采购、销售等有机会接触、利用重要或关键经营信息、技术信息或商业秘密的员工），可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；
e） 应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
f） 制义务，且保留验证核查记录；
g） 应提醒待录用的涉密人员，不应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，
h） 并保留提醒的记录，必要时得要求其签署不侵犯原任职机构商业秘密的承诺函。

9.1.2 员工履职管理

对于在职的人员，应采取以下管理措施：

a) 应要求所有员工熟悉并履行商业秘密管理制度及各项管理工作；
b) 应要求所有员工定期参与商业秘密保护的保密宣传及培训工作；
c) 应建立商业秘密管理奖惩制度，鼓励员工上报有关商业秘密管理体系、保密策略、保密措施
d) 等的漏洞，对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；
e) 应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；
f) 应督促岗位变动员工做好保密材料交接工作，对员工重新划分涉密类别与层级，及时做好涉
g) 密接触权限的调整；
h) 科研机构员工参加涉及商业秘密的工作会议等活动，应采取相应的保密措施。

9.1.3 员工兼职管理

对于兼职的人员，应采取以下管理措施：
a) 科研机构应制定员工对外从事兼职活动的管理办法，除了要求员工需遵守国家相关法律法规
b) 及政策性文件等规定外，还应遵守内部管理规定并履行相应的兼职审批程序；
c) 应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，建立兼职员工名册清单、
d) 在外兼职单位与参与外部项目清单；
e) 从事兼职活动的员工宜与科研机构、兼职单位三方共同签署兼职协议，以进一步明确兼职期
f) 限、各方保密义务以及知识产权权属或权利划分等约定；
g) 在无相关合同约定的情况下，应特别注意科研人员兼职研发工作与其在科研机构研发工作的
h) 隔离，包括但不限于研发过程所涉及的资源、文件、设备等物质技术条件的独立；
i) 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
j) 等证据资料；
k) 科研机构应不定期掌握科研人员在外兼职单位近期的商业秘密侵害风险，如该单位发生疑似
l) 涉入商业秘密或其他知识产权争议案件，应评估是否启动内部预警调查与列入警示名单。

9.1.4 员工离职管理

对于员工离职，应采取以下管理措施：
a) 涉密岗位员工离职前，应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
b) 法律责任。同时告知离职员工不应有以下行为：
   - 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、使用商业秘密等。
c) 应要求待离职涉密员工主动移交一切涉密载体和物品，并进行盘点和登记；
d) 应对待离职涉密员工（尤其对重点涉密人员）做好离职 IT 审计。离职 IT 审计宜包括但不限
e) 于以下内容：
   - 待离职涉密员工所使用的电脑上是否有权限之外的文档；
   - 待离职涉密员工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；
   - 待离职涉密员工所使用的信息系统，包括数据库或邮件系统等，其访问日志是否有异常；
   - 涉密员工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。
f) 宜主动探询待离职涉密员工该部门的其他同事，了解该员工离职原因是否有涉及竞争对手就
g) 业或其他可能涉及泄密窃密的风险因素；
h) 在涉密人员的离职审查过程中若发现其可能存在侵害商业秘密行为的，应及时收集并固定证
i) 据，然后按照泄密事件管理的规定处理；
j) 应对待离职涉密员工采取适当措施进行脱密，及时回收系统权限，并及时通知与离职员工有
k) 关的外部供应商、客户、合作单位等，做好业务交接；
l) 宜采取适当的方式或约定内容，进行离职人员追踪，尤其掌握已签订竞业限制协议的离职人
m) 员于竞业限制期限内的任职去向。

9.1.5 外部人员来访

对于外部来访人员，应采取以下管理措施：

a) 外部人员访问科研机构涉密区域应经审批，履行进出登记，且全程佩戴临时证件；
b) 外部人员进入涉密区域，受访部门应安排人员陪同，限制来访者使用具有录音、摄像、拍照、
c) 信息存储等功能的设备；
d) 外部人员进入涉密区域，应限制其使用网络接收、处理与传输信息的能力；
e) 科研机构与外部人员召开重要涉密会议，应主动告知相关保密义务与采取适当的保密措施；
f) 外部人员如需使用或外出携带商业秘密载体，无论是电子档案或是实体物品，均应由受访部
g) 门事先核实外部人员及其所任职的公司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内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。

9.1.6 科研机构实施涉密人员管理应有相应的计划文件、规范文件、程序文件及管理表单。

9.2 涉密文档管理

9.2.1 分级标示

对于涉密文档，应采取分级标示措施：

a) 科研机构应根据商业秘密的经济价值、技术重要性、管理效能与泄密后可能的风险危害程度
b) 等因素进行评估，将商业秘密载体进行分级管理；
c) 商业秘密载体分级见表 1；
d) 商业秘密载体应标记相应的提示警语文字与密级标识，任何人不得私自删除、涂改或遮蔽商
e) 业秘密文件的密级标识；
f) 科研机构应严格要求员工落实分级与标示，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
“内部限阅”（Restricted）	指仅限本科研机构内部传阅，较不具有敏感性的信息。
“一般商业秘密”（Confidential）	指仅能在有权限的人员范围内流转，一旦泄露，可能威胁到科研机构的研究发展，削弱市场竞争力，对科研机构经济利益造成一般损失、危害和影响的商业秘密。
“核心商业秘密”（Top Secret）	指一旦泄露，立刻威胁到科研机构的生存及发展，严重削弱核心竞争力，对经济利益造成特别严重损失、危害和影响的商业秘密。

9.2.2 储存保管

对于涉密文档储存保管，应采取以下管理措施：

a) 对于涉密文档，应采取以下储存保管措施：各涉密部门应指定专人负责该部门的商业秘密载
b) 体存档和保管工作；
c) 科研机构应定期对商业秘密载体进行备份；
d) 商业秘密载体应存放在科研机构监管下的实体储存处或指定的信息系统。宜避免员工在办公
e) 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，应事先提交相关申请，且获得涉密部门主管审批同意；
f) 实体形式的商业秘密载体保存方式宜与其他一般文件或物品有所区隔，或使用上锁的储物柜，
g) 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；

h） 科研机构存放商业秘密载体的区域应配备监控摄像头、火灾报警等安防设备。

9.2.3 内部流通

对于涉密文档内部流通，应采取以下管理措施：

a） 应规定与限制所有员工使用商业秘密载体的场地、时机、条件、设备与方式；
b） 科研机构应规定员工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
c） 项目转移、披露或使用之前，需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；
d） 应规定员工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、
e） 储存系统、收发件流程或密封包（箱）等；
f） 商业秘密载体的请求与交付过程，均应以基于仅需要知道的原则（Need To Know Basis）审
g） 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，不宜进行接触或流通；
h） 宜制定标准化的档案命名与版本编号等原则，易于员工快速辨识与遵守实施；
i） 科研机构对于员工实际接触商业秘密载体或密点信息的行为宜保有操作日志或相关记录。

9.2.4 加密保护

对于涉密文档加密保护，应采取以下管理措施：

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
b） 外恢复还原等安全管理措施；
c） 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
d） 方案等。

9.2.5 删除销毁

对于涉密文档删除销毁，应采取以下管理措施：

a） 所有员工不得随意弃置、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，应由涉密部门专责人员列出销毁
c） 清单与事由，经商业秘密管理组织审批后实施；
d） 商业秘密信息载体的销毁过程应采取监督措施，如视频监控、录像、见证；
e） 应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。

9.2.6 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、加解密及销毁等应保留记录；
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。

9.2.7 科研机构实施涉密文件管理应有相应的计划文件、规范文件、程序文件及管理表单。

9.3 涉密系统管理

9.3.1 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） 应视业务或任务需求，为员工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
b） 和密码；
c） 账号和密码属于个别员工且仅限本人保管使用，不得与其他员工共用；
d） 应避免使用默认密码或保存密码等方式自动登录信息系统；
e） 应制定账号命名规则，且账号内容宜包括特殊符号、大写英文字母、小写英文字母、数字四
f） 种不同字符。账号名称应避免使用易于猜测或广为人知的常用字词；
g） 应制定密码强度（长度）规则，且密码内容宜包括特殊符号、大写英文字母、小写英文字母、

h） 数字四种不同字符；密码应避免使用易于猜测或广为人知的常用字词；
i） 信息系统账号的初始密码应是随机产生；
j） 信息系统的密码应通过系统设置强制用户定期更换；
k） 应设置账号或密码登录错误的次数限制，超过限制即应立即锁定该账号，并了解原因；
l） 如有业务部门需设置公用账号、匿名账号等特殊账号，则应经过商业秘密管理组织审批；
m） 信息系统的账号密码应建立申请、登记、审核、发放及撤销等作业办法，由专人负责管理并
n） 保留所有变更记录。

9.3.2 权限管理

对于涉密系统权限管理，应采取以下管理措施：

a） 应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） 应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） 应对员工接触商业秘密信息的相关涉密系统，如办公电脑设备、数据库和各类应用系统，为
d） 其账户实行权限管理，以“最小够用”原则设定权限；
e） 涉密系统的权限应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
f） 围等；
g） 如有权限到期、人员变更、转岗或离职、项目变更等情况，应及时变更、撤销相应的信息系
h） 统权限；
i） 信息系统的权限变更事件应保留完整记录日志；
j） 信息系统的管理员权限应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
k） 系统的情况。

9.3.3 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员工公务使用，且作为主要的商业秘密信息处理设备；
b） 员工携带个人电脑至科研机构办公，应由商业秘密管理组织审批核定。科研机构可视员工职
c） 务涉密程度与权限层级，要求限制员工个人电脑的信息处理能力，包括但不限于不得于本地端储存商业秘密载体、不得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等；
d） 除非是员工执行业务所必需的硬件功能，否则宜关闭或禁用办公电脑的移动存储、光驱、蓝
e） 牙、无线网卡等数据传输功能模块，以及摄像头、声卡、话筒等音视频采集设备；
f） 办公电脑硬件的配置、维修、报废均应经过审批或授权交由指定人员处理，应使用封条封住
g） 主机以禁止员工私自拆机维修、更换、增加硬件配件；
h） 办公电脑未经批准不得安装非授权软件；
i） 办公电脑的网络接入、网络配置均应按规定设置，禁止接入非授权网络；
j） 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；
k） 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。

9.3.4 数据系统

对于涉密数据系统，应采取以下管理措施：

a） 商业秘密载体应存储于科研机构授权的数据系统，不应存储于非授权的存储设备或网络空间；
b） 员工应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） 员工操作数据系统时，以下行为应履行审批手续，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） 科研机构应保存员工使用数据系统的操作记录；
e） 数据系统应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） 数据系统应有相应的信息安全保护机制，如防火墙、杀毒软件等；
g） 数据系统应定期进行备份以及信息安全漏洞检测；
h） 数据系统应有相应的灾害应变与系统复原措施。

9.3.5 智能手机

对于涉密智能手机，应采取以下管理措施：

a） 应评估实际需求，列册核发专用的智能手机，供员工执行业务使用；
b） 科研机构核发的智能手机应由专人专管专用，且事先安装具有身份识别、内容加密、设备绑
c） 定、行为监控等保密措施的软件；
d） 员工个人智能手机不宜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
e） 商业秘密信息；
f） 员工个人智能手机不应接入科研机构涉密网络。

9.3.6 移动存储

对于涉密移动存储，应采取以下管理措施：

a） 科研机构应评估实际需求，列册核发专用的涉密移动存储设备，供员工执行业务使用；
b） 涉密移动存储设备应由专人专管专用，且使用具有身份识别、内容加密、设备绑定、行为监
c） 控等保密功能的设备；
d） 员工完成任务后应缴回涉密移动存储设备且确实清空存储内容；
e） 未经审批不得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得连接非涉密或未
f） 采取保密措施的计算机及电子设备；
g） 未经审批不得携出涉密移动存储设备至科研机构外部使用。

9.3.7 信息传输

对于涉密信息传输，应采取以下管理措施：

a） 应限制员工进行商业秘密载体传输或交换的渠道，包括但不限于以下几种方式：
  - 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） 员工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，应于信息内文加注提示警语
c） 文字与密级标识，必要时得以加密方式进行档案传输；
d） 员工收到疑似非经授权或许可的商业秘密载体或涉密信息时，应主动通报事业单位主管或商
e） 业秘密管理组织，不得进一步接触或使用该涉密档案；
f） 科研机构的办公网络不应允许员工访问非科研机构邮箱的外部邮箱，应将常见的外部邮箱、
g） 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应经过审批并备案邮箱账号和密码；
h） 应禁止员工使用私人网盘，应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
i） 网盘的应经过审批，并向科研机构备案网盘账号和密码；
j） 科研机构办公电脑使用的即时通讯软件应避免和其他外部通讯软件交互商业秘密信息；
k） 对于涉密信息的传输，科研机构应具备权限管理、操作记录日志与行为监控等保密能力。

9.3.8 科研机构实施涉密系统管理应有相应的计划文件、规范文件、程序文件及管理表单。

9.4 涉密区域管理

9.4.1 科研机构内部的办公区域应根据事业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。

9.4.2 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) 员工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，需经业务部门主管
c) 审批取得临时授权；
d) 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」等警语标识；
e) 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；
f) 宜限制员工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；
g) 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；
h) 应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；
i) 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；
j) 涉密电脑屏幕可配备防偷窥、防拍照措施；
k) 较高等级的涉密区域可评估是否应适时关闭或遮蔽对外窗户，以避免外部窥视；
l) 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；
m) 非经业务部门主管审批同意，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
n) 密区域内的物品或设备，应保留携出登记记录。

9.4.3 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。

9.4.4 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应使用终端准入限制、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。

9.4.5 科研机构需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。

9.4.6 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) 科研机构应制定共享平台物理环境管理规范及使用规定；
b) 共享平台应设置专职管理员，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
c) 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，标签内容应包括设备责任人和紧急联系电话等；
d) 科研机构应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；
e) 共享平台所有设备与物理环境应与科研机构涉密区域进行隔离，外部使用人员不得接入可能
f) 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；
g) 外部使用人员每次使用共享平台后，应自行保存实验研究成果。每次使用结束后，应由专职
h) 管理员进行设备检查并进行清空还原；
i) 专职管理员应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。

9.4.7 科研机构实施涉密区域管理应有相应的计划文件、规范文件、程序文件及管理表单。

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，可能包括但不限于以下几种方式：

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敏感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敏感信息，适度进行遮挡或隐蔽。

10.1.4 科研机构信息公开的保密工作应有相应的计划文件、规范文件、程序文件及管理表单。

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，应评估窃密风险，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，确实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管道的敏感信息。

10.2.5 科研机构商务活动的保密工作应有相应的计划文件、规范文件、程序文件及管理表单。

10.3 委外服务

10.3.1 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。

10.3.2 科研机构委外服务的保密工作应有相应的计划文件、规范文件、程序文件及管理表单。

10.4 科技成果转化

10.4.1 科研机构进行科技成果转化，包括但不限于以下形式：
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 不论以何种方式实施科技成果转化，都应依法签订合同，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。

10.4.3 科研机构应依照科技成果转化合同所约定的内容、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。

10.4.4 若科技成果转化合同因故终止或发生争议事项，科研机构应立即通知签约对象暂停或终止继续使用商业秘密的权利，相关措施包括但不限于要求返还已交付的商业秘密涉密文件或禁止散播流通。前述告知事项应确认签约对象书面同意且保有完整的记录。

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　科研机构商业秘密管理体系的检查与改进应有相应的计划文件、规范文件、程序文件及管理表单。

11.7　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。

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 29490－2013 企业知识产权管理规范

[3] GB/T 33250－2016 科研组织知识产权管理规范

[4] GB/T 22239－2019 信息安全技术 网络安全等级保护基本要求

[5] DB33/T 2273—2020 商业秘密保护管理与服务规范

[6] DB4403/T 235－2022 企业商业秘密管理规范

[7] DB43/T 2652－2023 企业商业秘密保护管理规范

[8] SF/T 0076—2020 电子数据存证技术规范

[9] T/PPAC 701—2021 企业商业秘密管理规范

[10] T/SHSFJD 0001—2020 基于区块链技术的电子数据存证规范

[11] T/CESA 1048—2018 区块链存证应用指南

[12] 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

[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

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

[15] 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

[16] 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

[17] 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司法解释》：法释〔2004〕19号.2020年

[18] 最高人民法院.《人民法院在线诉讼规则》：法释〔2021〕12号.2021年

[19] 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

[20] 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

[21] 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

[22] 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（十二）:中华人民共和国主席令第18号.2023年

[23] 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