ICS 03.100.01
CCS A 01

T/ASIA

安 徽 省 软 件 行 业 协 会 团 体 标 准

T/ASIA 0001—2024

软件行业商业秘密保护规范

Specification for Trade secrets Protection in the Software Industry

2024－01－26 发布　　2024－02－01 实施

安徽省软件行业协会　　发 布

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。

本文件由科大国创软件股份有限公司提出。

本文件由安徽省软件行业协会归口。

本文件起草单位：科大国创软件股份有限公司、安徽宝葫芦集团信息科技集团股份有限公司、中通服和信科技有限公司、安徽华米信息科技有限公司、合肥美亚光电技术股份有限公司、合肥金星智控科技股份有限公司、合肥泰禾智能科技集团股份有限公司、中水三立数据技术股份有限公司、安徽中鑫继远信息技术股份有限公司、安徽芯纪元科技有限公司、安徽亘达信息科技有限公司、合肥高新区市场监督管理局、安徽省质量和标准化研究院。

本文件主要起草人：高品、刁海娟、张正全、张雪晨、王春兰、申远、曾燕、穆宣临、李岳民、余第喜、汪家常、李清、王润杰、胡冠宇、陶学明、董先权、卢淑芳。

软件行业商业秘密保护规范

1 范围

本文件规定了软件行业商业秘密保护的术语和定义、总体要求、组织领导、商业秘密的管理、涉密事项的管理、应急准备与响应、检查与改进等内容。

本文件适用于软件行业商业秘密的保护工作。

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。

DB34/T 4317 商业秘密保护规范

DB34/T 4533 企业商业秘密管理体系 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，对所有权人具有现实或潜在的竞争优势，能够为所有权人带来经济效益、具有实用性，或经权利人采取相应的保密措施的技术信息和经营信息商业信息；一旦泄露，会对权利人（所有权人）产生一定的经济损失和丧失现实或潜在的市场竞争优势或机会。

3.2

涉密载体 secret-related carriers

以文字、数据、符号、图形、图像、视频和音频等形式记载或存储商业秘密信息的各类物质，如纸质介质、存储介质（U盘、硬盘、光盘、服务器等）和其他介质。

3.1

涉密物品 secret-related items

含有商业秘密信息的设备、原材料、半成品和样品等。

3.2

涉密设备 secret-related device

生成、存储、处理商业秘密的设备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。

3.3

涉密区域 secret-related area

可以接触到商业秘密信息的场所，包括但不限于企业园区、厂房、车间、实验室、办公室、保密室、档案室、机房、用户现场等。

4 总体要求

4.1 企业应坚持“企业自主、预防为先、依法维权”的商业秘密保护原则。

4.2 企业应建立商业秘密保护机制，建立商业秘密保护机构，配备专（兼）职保密人员。

4.3 企业应配备满足商业秘密保护所需的设施和设备。

4.4 企业应建立健全商业秘密保护管理制度，并按制度要求实施管理工作。

4.5 企业应组织开展商业秘密保护相关法律法规、制度等知识的学习培训，不断提高人员的保密意识和商业秘密的保护能力。
4.6 企业宜按照 DB34/T 4533 的要求，建立、实施并持续改进商业秘密管理体系，将商业秘密管理贯彻到企业的全部经营活动过程。

5 组织领导

5.1 企业应根据实际需要建立商业秘密保护委员会或领导小组，成员宜包括最高管理者、涉密部门的负责人等，其工作职责包括但不限于：

a) 建立商业秘密管理方针和目标；
b) 将商业秘密管理要求整合到企业的业务中；
c) 要求员工加强商业秘密保护意识；
d) 管理并支持员工为商业秘密管理体系的实施持续努力；
e) 促进商业秘密管理体系的持续改进。

5.2 企业应根据实际需要设立商业秘密保护办公室，或指定知识产权管理部门或法务部门开展商业秘密的保护工作，应配备专职负责人，或者指定某一部门负责人兼任，并配备专职或兼职保密工作人员，其中 1 名应为保密技术管理人员。其工作职责包括但不限于：

a) 落实保密管理和技术防范措施；
b) 制定保密制度；
c) 确定涉密岗位级别；
d) 建立商业秘密保护的责任制；
e) 审批确定企业文件密级；
f) 形成企业各密级文件清单；
g) 保持动态管理；
h) 负责检查指导企业商业秘密工作情况。

6 商业秘密的管理

6.1 总则

6.1.1 企业商业秘密的管理应由商业秘密保护委员会或领导小组统一组织实施。
6.1.2 企业应制定商业秘密管理制度，明确商业秘密的定密、隐秘、解密、销秘等工作的准则或程序。
6.1.3 企业应按照规定准则或程序对商业秘密的定密、隐秘、解密、销秘等过程实施管理，并保留过程管理的成文信息。

6.2 定密

6.2.1 定密范围

企业商业秘密保护委员会或领导小组应界定其商业秘密的定密范围，定密范围宜考虑以下方面：

a) 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技术信息；
b) 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、数据等经营信息。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；
c) 符合商业秘密构成要件，除技术信息、经营信息以外的商业信息。

6.2.2 定密要求

6.2.2.1 涉密部门或涉密个人应及时收集和登记生产经营过程中产生的技术信息、经营信息等商业信息，拟定保密项目，并填写定密申请，经部门保密负责人签批确认后，报送企业商业秘密管理办公室。
6.2.2.2 商业秘密管理办公室牵头组建定密小组，定密小组对提出的商业秘密确认申请进行论证，论证内容包括但不限于：

a) 密点的公众知悉或获取渠道。此时需要论证包括但不限于以下情况：
   1) 未在国内外公开使用；
   2) 未在国内外公开出版物或者其他媒体上公开披露；
   3) 未通过公开的报告会、展览等方式公开；
   4) 不属于其所属领域相关人员普遍掌握的常识或行业惯例；
   5) 不能仅涉及产品尺寸、结构、材料、部件的简单组合等内容；
   6) 不能从公开渠道获得。
b) 密点的现实的或者潜在的商业价值。此时需要论证包括但不限于以下情况：
   1) 给企业带来的经济收益，包括现有的和潜在的经济收益；
   2) 对企业生产经营的重要程度；
   3) 企业的投入研发、经营以及其他成本；
   4) 为企业带来竞争优势；
   5) 竞争对手获取商业信息后产生的价值；
   6) 因信息泄露后产生或可能产生的经济损失；
   7) 因信息泄露后可能承担的法律责任。

6.2.2.3 经论证的商业秘密，由商业秘密管理办公室统一报送企业保密委员会或领导小组审批确定。企业可通过公证、第三方存证、电子存证等证据保全方式实现对商业秘密权属的初步确认。

6.2.2.4 企业应根据商业秘密的重要性程度和商业价值高低，确定商业秘密的密级，一般划分为核心商业秘密、重要商业秘密、一般商业秘密和定向商业秘密。各密级划分标准如下：

a) 核心商业秘密是指公开或泄露后，会给权利人带来致命的、毁灭性的、长久性极大伤害或即时性持续重大伤害或极大经济损失的商业秘密。
b) 重要商业秘密是指公开或泄露后，会给权利人带来相对滞后的持续性重大伤害或短期性即时重大伤害或重大经济损失的商业秘密。
c) 一般商业秘密是指较难采取技术和物理防护措施，且公开或泄露后会给权利人带来相对滞后的持续性较大伤害或即时性一般伤害或一般经济损失的商业秘密。
d) 定向商业秘密是指无法采取技术和物理防护措施，且被竞争对手、同业人员或特定的利益相关者知悉后，给权利人带来伤害、经济损失、竞争威胁、潜在负面影响的商业秘密。

6.2.2.5 商业秘密管理办公室应对审批后的商业秘密及其相关文件进行登记备案，并明确其密级、保密期限、知悉范围、保密事项、保护措施、存放地点及保存方式等内容。

6.3 隐密

6.3.1 下列情形涉及商业秘密的，应由定密小组对相关信息予以隐藏：

a) 与供应商、客户、合作方等的沟通和信息往来中；
b) 信息公开、发布、流转时；
c) 协助其他单位尽职调查时；
d) 其他情形。

6.3.2 可采取的隐密方式包括但不限于：

a) 隐藏或删除涉密信息；
b) 对涉密信息进行模糊化处理；
c) 其他方式。

6.4 解密

6.4.1 满足下列要求之一的商业秘密，应由定密小组对其进行解密：

a) 企业认为商业秘密事项已不再具有保护价值的；
b) 保密期限届满；
c) 其它特定因素导致商业秘密被公开的。

6.4.2 可采取的解密方式包括但不限于：

a) 移出涉密区域；
b) 消除密级标识、提示；

c） 电子文档解密；
d） 其他方式。

6.5 销密

6.5.1 销毁涉及商业秘密的文件(含复制文件)、资料、电子信息、载体和物品，应列出销毁清单，经商业秘密保护办公室审批后，由定密小组实施。可采取的销毁方式包括但不限于：

a） 文件、资料应粉碎成颗粒状或焚烧处置；
b） 电子信息应利用彻底删除软件永久删除；
c） 含有核心秘密的电子信息载体应做销毁处理；
d） 其他合适的方式。

6.5.2 可采取下列方式对销毁过程进行监督管理：

a） 在视频监控范围内销毁；
b） 不少于 2 名定密人员见证下销毁；
c） 对销毁过程录像等。

6.6 标志

6.6.1 企业商业秘密的标志由密级、标识、保密期限三部分组织，标志以 3 号方正黑体字。示例：“绝密 R 15 年”。

6.6.2 涉密文件应将标志标注在文件首页左上角。涉密载体应在外包装上标明与内容一致的密级。标志与涉密载体不得分离。

6.6.3 摘录、引用秘密信息的，应在派生载体上标识与原件一致的密级。

6.6.4 文件资料汇编中有涉密文件的，除对各独立文件的密级做出标识外，还应按照汇编中的最高密级，在封面做出标识。

6.6.5 各部门对商业秘密标识后，应即行登记建立台帐，由专人管理，按企业档案管理有关规定建立查阅、借阅制度。

6.6.6 在特殊情况下，未进行标识的涉密资料、涉密文件仍然为商业秘密。

7 涉密事项的管理

7.1 涉密人员管理

企业应对涉密人员进行保密管理：

a） 应制定涉密人员管理制度，明确涉密人员的应聘、入职、在职、离职等环节的管理要求，定期或不定期对涉密人员进行识别和登记。
b） 应对涉密岗位的应聘人员进行保密事项提醒，对涉密岗位的拟入职人员进行背景调查；应要求其做出不侵犯前雇主的商业秘密、不违反与前雇主签订的竞业限制协议等承诺；
c） 应与新入职员工签署保密协议，约定保密范围、双方的权利和义务、违约责任等。必要时，可签署竞业限制协议；开展新入职人员的保密教育培训，培训结束后并进行考核，保存培训和考核记录；
d） 应对在职人员进行管理，建立涉密人员名单，实施分级管理；定期开展保密教育培训，对其履行职责情况进行检查和考核；实时关注人员岗位变动情况，做好保密工作和材料交接，进行涉密接触权限的调整；
e） 应对涉密人员离职进行管理，对其使用的涉密设备、涉密载体、涉密文件及相关物品进行清查并移交；开展离职面谈，告知其离职后应负有的保密义务；应完成涉密载体的交接，开展离职涉密审查，签署保密承诺书；宜对其离职后的去向进行追踪；
f） 应对聘任或委托外聘的专家、顾问、翻译、律师等可能接触涉密信息的外部人员签订保密协议或保密承诺书，宜进行背景调查；临时访问人员需要接触或可能接触商业秘密时，应经审批和登记，签订保密协议或保密承诺书，并安排保密人员全程陪同。

企业应保留涉密人员管理的成文信息。

7.2 涉密载体管理

企业应对涉密载体进行保密管理：

a） 应制定涉密载体管理制度，明确涉密载体的识别和确定、制作、使用、保存、维修和销毁等环节的管理要求；

b） 应识别和确定企业所有涉密载体，建立涉密载体台账，宜按照涉密信息的密级和性质进行分类，实行分级管理；应定期对涉密载体进行清点和核查，确定涉密载体的数量、位置、状况等信息；

c） 涉密载体制作过程应进行保密，由专人负责制作、收转、存档，并在涉密载体的适当位置标注涉密标志；秘密载体宜在本单位制作，委托外单位制作应事前签订保密协议；

d） 涉密载体的使用（包括查阅、借阅、复印、拷贝等）应履行审批和登记手续，并对涉密载体的流转过程进行记录；

e） 涉密载体应保存在涉密区域的专用设备中，并由专人负责保管；涉密载体的维修，应指定专人全程现场监督；

f） 涉密载体的维修和销毁应履行审批和登记手续，按照规定的程序和方法，并在专人监督下进行。

应保留涉密载体管理的成文信息。

g） 对于电子涉密载体(如U盘)应该进行数据加密，密钥和涉密载体分开存储，涉密载体密钥应由专人管理并定期更新。

7.3 涉密物品管理

企业应对涉密物品进行保密管理：

a） 应制定涉密物品管理制度，明确涉密物品的识别和确定、生产和加工、使用、保存、维修和销毁等环节的管理要求；

b） 应识别和认定企业所有涉密物品，建立涉密物品台账，宜实行分级管理，并在醒目位置粘贴（悬挂）涉密指示标识和禁止行为的警示标识；应定期对涉密物品进行清点和核查，确定涉密物品的数量、位置、状况等信息；

c） 应在涉密区域内进行涉密物品的生产和加工，宜根据涉密物品生产和加工流程，安排不同的人员负责不同的环节；

d） 应在涉密区域内使用涉密物品，并履行使用登记程序；对外销售的涉密物品，应与客户签订保密协议或在销售合同中增加保密义务条款，宜采取足以对抗不特定第三人通过反向工程获取其技术秘密的保护措施；

e） 应在指定的涉密区域存放涉密物品，并指定专人负责管理；

f） 涉密物品的维修、报废应履行审批和登记手续，按照规定的程序和方法，并在保密人员监督下进行。

应保留涉密物品管理的成文信息。

7.4 涉密区域管理

企业应对涉密区域进行保密管理：

a） 应制定涉密区域管理制度，明确涉密区域的识别和确定、安全防护、日常管理、检修和维护等环节的管理要求；

b） 应识别企业所有涉密区域，确定涉密区域的范围，并在醒目位置粘贴（悬挂）涉密区域指示标识和禁止行为的警示标识；宜根据区域内涉密物品、涉密信息及其载体的密级和性质，划分涉密区域的保密级别，实施分级管理；

c） 应对涉密区域进行物理隔离，并根据其保密级别，选择安装安全防范设施设备，配备专职安保人员和管理人员；

d） 涉密区域内部使用的通信、网络、计算机、信息系统、办公设备等应符合国家相关保密规定和技术标准的要求；

e） 应对涉密区域人员、物资进出实行登记管理，未经审批或授权严禁人员进入和物资离开；涉密区域如需接待外来人员，应指派保密人员全程陪同，并告知保密注意事项和要求；必要时，应进行安全检查，限制携带或使用具有录音、摄像、拍照、信息存储等功能的设备；

f） 应定期对涉密区域的设施设备进行检修和维护，并履行审批和登记手续，按照规定的程序和方法，并在保密人员监督下进行；必要时，应开展不定期巡查工作。

g)在涉密区域应佩戴明确反应当前人员身份的身份牌，可以根据颜色来反应当前人员是内部涉密人员和外来人员。在涉密区域发现未佩戴身份牌或外来人员无陪同人员时，内部涉密员工应该及时进行干预并告知涉密区域管理员。身份牌的发放和回收由专人进行台账登记管理。

应保留涉密区域管理的成文信息。

7.5 涉密商务活动管理

企业应对涉密商务活动进行管理：

a） 应制定涉密商务活动管理制度，明确涉密商务活动中信息发布、涉密会议、商业活动、对外合作、产权交易等活动的管理要求；

b） 应对信息发布实施保密审查，明确人员职责权限，对新闻稿件、展览展会宣传资料、著作论文、申请专利等信息实施对外发布前审查、发布后检查，以及对涉密信息的追踪；

c） 应对涉密会议实施商业秘密管理，选择具有保密条件的场所，限定参会人员范围，签订保密协议或承诺书；涉密文件资料应有明显保密和会后回收标识，会后应及时收回、清点和登记。

d） 应对涉密的采购、销售、委托开发、委托生产、参展等商业活动实施商业秘密管理，开展相关方的保密能力评价，签订保密协议，定期或不定期对相关方进行保密监督检查；

e） 应对技术合作、商务合作、共同研究等对外合作实施保密管理，签订合作合同，约定原始商业秘密以及在共同开发、改进或二次开发中形成的商业秘密的内容、归属、管理责任和保密义务；

f） 应对企业并购或重组、技术许可或转让等产权交易活动实施商业秘密管理，清理和登记现有商业秘密，形成清单，并采取相应保密措施；记录涉密人员去向。

应保留涉密商务活动管理的成文信息。

8 应急准备与响应

8.1 应急准备

企业应建立、实施并保持对商业秘密潜在的紧急情况进行应急准备，包括响应所需的过程：

a） 针对商业秘密泄密、侵权等紧急情况策划应急预案；

b） 为所策划的响应提供培训；

c） 定期对策划的应急预案进行测试或演练；

d） 定期评审并修订过程和策划的响应措施，特别是发生紧急情况后或进行试验后。

企业应保留关于响应潜在紧急情况的过程和计划的成文信息。

8.2 应急响应

8.2.1 企业应对已发生的泄密、侵权等紧急情况做出响应，包括但不限于：

a） 启动对商业秘密泄漏、侵权等紧急事件的核查，确认事件发生的事实和过程；

b） 分析商业秘密泄漏或侵权原因，判断是否侵权，并评估事件的严重程度；

c） 收集和固定商业秘密相关证据；必要时，可委托律师调查取证、通过公证机构取证、向法院申请证据保全和/或申请法院调查取证；

d） 依法开展维权，可按照 DB34/T 4317 的规定，向市场监督管理部门、公安机关、人民法院、人民检察院等寻求行政保护和司法保护。

8.2.2 企业可视不同侵权情况，采取不同的方式进行维权：

a） 双方协商和解。当商业秘密侵权情节轻微，双方通过自行协商并达成和解；

b） 申请调解。当发生商业秘密侵权纠纷，且尚未经过法院、公安或者其他行政机关受理，双方可向人民调解委员会等调解组织申请民事纠纷调解；

c） 申请仲裁。若双方达成商业秘密相关仲裁协议或合同中有仲裁规定，双方可根据协议规定，向仲裁委员会申请经济纠纷仲裁；

d) 寻求行政保护。权利人有证据表明其商业秘密受到侵犯，可首先向县级以上市场监督管理部门举报，由市场监督管理部门进行认定查处；
e) 寻求司法保护。当发生侵犯商业秘密，给企业造成损失数额在30万元以上的，或者因侵犯商业秘密违法所得数额在30万元以上的，或者直接导致企业经营困难而破产、倒闭等其他重大经济损失的，企业可直接向公安机关举报，依法追究侵权人的刑事责任；企业还可以向人民法院提起民事诉讼，要求侵权人停止侵权并赔偿相应损失。

8.2.3 企业寻求行政或司法保护时，应主动提供包括但不限于以下材料：
a) 商业秘密权利人主体资格；
b) 商业秘密的法定构成要件，包括该商业秘密的产生过程、载体、具体秘密点内容、商业价值、不为公众所知悉以及对其采取的具体保密措施等；
c) 被举报人主体资格及其具有接触或实施侵犯该商业秘密行为的相关证明材料；
d) 被举报人使用的商业信息与请求人请求保护的商业秘密具有共同或类似商业价值的证明材料；
e) 其他表明商业秘密被侵犯的证据。

9 检查与改进

9.1 企业应建立并实施商业秘密保护监督检查和改进制度，明确监督检查的内容和方法、职责和权限、频次与时限、改进要求等。

9.2 商业秘密保护办公室负责定期组织对商业秘密保护情况进行检查，对发现的问题提出整改要求，并监督落实。

9.3 商业秘密泄露事件发生后，商业秘密保护领导小组应当组织对泄密事件进行专门评估，并根据评估结果对商业秘密保护体系进行改进。

9.4 企业应强化监督检查结果运用，建立完善商业秘密保护奖惩激励、应急处置等日常工作机制。