商业秘密

保护指导手册（2025）

金杜律师事务所
KING&WOOD MALLESONS

Linemore 蓝盟

目录

第一部分 商业秘密保护法律法规

1.1 法律法规

1.1.1 中华人民共和国反不正当竞争法（2019 年修正）

第九条 经营者不得实施下列侵犯商业秘密的行为

（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；

（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；

（四）教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密。

第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

本法所称的商业秘密，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。

第三十二条 在侵犯商业秘密的民事审判程序中，商业秘密权利人提供初步证据，证明其已经对所主张的商业秘密采取保密措施，且合理表明商业秘密被侵犯，涉嫌侵权人应当证明权利人所主张的商业秘密不属于本法规定的商业秘密。

商业秘密权利人提供初步证据合理表明商业秘密被侵犯，且提供以下证据之一的，涉嫌侵权人应当证明其不存在侵犯商业秘密的行为：

（一）有证据表明涉嫌侵权人有渠道或者机会获取商业秘密，且其使用的信息与该商业秘密实质上相同；

（二）有证据表明商业秘密已经被涉嫌侵权人披露、使用或者有被披露、使用的风险；

（三）有其他证据表明商业秘密被涉嫌侵权人侵犯。

1.1.2 中华人民共和国促进科技成果转化法（2015 年修正）

第三条 科技成果转化活动应当尊重市场规律，发挥企业的主体作用，遵循自愿、互利、公平、诚实信用的原则，依照法律法规规定和合同约定，享有权益，承担风险。科技成果转化活动中的知识产权受法律保护。

第十一条 国家建立、完善科技报告制度和科技成果信息系统，向社会公布科技项目实施情况以及科技成果和相关知识产权信息，提供科技成果信息查询、筛选等公益服务。公布有关信息不得泄露国家秘密和商业秘密。对不予公布的信息，有关部门应当及时告知相关科技项目承担者。

第十九条 科技成果完成人或者课题负责人，不得阻碍职务科技成果的转化，不得将职务科技成果及其技术资料和数据占为己有，侵犯单位的合法权益。

第三十条 国家培育和发展技术市场，鼓励创办科技中介服务机构，为技术交易提供交易场所、信息平台以及信息检索、加工与分析、评估、经纪等服务。

科技中介服务机构提供服务，应当遵循公正、客观的原则，不得提供虚假的信息和证明，对其在服务过程中知悉的国家秘密和当事人的商业秘密负有保密义务。

第四十条 科技成果完成单位与其他单位合作进行科技成果转化的，应当依法由合同约定该科技成果有关权益的归属。合同未作约定的，按照下列原则办理：

（一）在合作转化中无新的发明创造的，该科技成果的权益，归该科技成果完成单位；

（二）在合作转化中产生新的发明创造的，该新发明创造的权益归合作各方共有；

（三）对合作转化中产生的科技成果，各方都有实施该项科技成果的权利，转让该科技成果应经合作各方同意。

第四十一条 科技成果完成单位与其他单位合作进行科技成果转化的，合作各方应当就保守技术秘密达成协议；当事人不得违反协议或者违反权利人有关保守技术秘密的要求，披露、允许他人使用该技术。

第四十二条 企业、事业单位应当建立健全技术秘密保护制度，保护本单位的技术秘密。职工应当遵守本单位的技术秘密保护制度。

企业、事业单位可以与参加科技成果转化的有关人员签订在职期间或者离职、离休、退休后一定期限内保守本单位技术秘密的协议；有关人员不得违反协议约定，泄露本单位的技术秘密和从事与原单位相同的科技成果转化活动。

职工不得将职务科技成果擅自转让或者变相转让。

第四十八条 科技服务机构及其从业人员违反本法规定，故意提供虚假的信息、实验结果或者评估意见等欺骗当事人，或者与当事人一方串通欺骗另一方当事人的，由政府有关部门依照管理职责责令改正，没收违法所得，并处以罚款；情节严重的，由工商行政管理部门依法吊销营业执照。给他人造成经济损失的，依法承担民事赔偿责任；构成犯罪的，依法追究刑事责任。

科技中介服务机构及其从业人员违反本法规定泄露国家秘密或者当事人的商业秘密的，依照有关法律、行政法规的规定承担相应的法律责任。

第五十条 违反本法规定，以唆使窃取、利诱胁迫等手段侵占他人的科技成果，侵犯他人合法权益的，依法承担民事赔偿责任，可以处以罚款；构成犯罪的，依法追究刑事责任。

第五十一条 违反本法规定，职工未经单位允许，泄露本单位的技术秘密，或者擅自转让、变相转让职务科技成果的，参加科技成果转化的有关人员违反与本单位的协议，在离职、离休、退休后约定的期限内从事与原单位相同的科技成果转化活动，给本单位造成经济损失的，依法承担民事赔偿责任；构成犯罪的，依法追究刑事责任。

1.1.3 中华人民共和国民法典

第一百二十三条 民事主体依法享有知识产权。

知识产权是权利人依法就下列客体享有的专有的权利：

（一）作品；

（二）发明、实用新型、外观设计；

（三）商标；

（四）地理标志；

（五）商业秘密；

（六）集成电路布图设计；

（七）植物新品种；

（八）法律规定的其他客体。

第四百四十条 债务人或者第三人有权处分的下列权利可以出质：

（一）汇票、本票、支票；

（二）债券、存款单；

（三）仓单、提单；

（四）可以转让的基金份额、股权；

（五）可以转让的注册商标专用权、专利权、著作权等知识产权中的财产权；

（六）现有的以及将有的应收账款；

（七）法律、行政法规规定可以出质的其他财产权利。

第五百零一条 当事人在订立合同过程中知悉的商业秘密或者其他应当保密的信息，无论合同是否成立，不得泄露或者不正当地使用；泄露、不正当地使用该商业秘密或者信息，造成对方损失的，应当承担赔偿责任。

第六百条 出卖具有知识产权的标的物的，除法律另有规定或者当事人另有约定外，该标的物的知识产权不属于买受人。

第八百五十一条 技术开发合同是当事人之间就新技术、新产品、新工艺、新品种或者新材料及其系统的研究开发所订立的合同。

技术开发合同包括委托开发合同和合作开发合同。

技术开发合同应当采用书面形式。

当事人之间就具有实用价值的科技成果实施转化订立的合同，参照适用技术开发合同的有关规定。

第八百五十二条 委托开发合同的委托人应当按照约定支付研究开发经费和报酬，提供技术资料，提出研究开发要求，完成协作事项，接受研究开发成果。

第八百五十三条 委托开发合同的研究开发人应当按照约定制定和实施研究开发计划，合理使用研究开发经费，按期完成研究开发工作，交付研究开发成果，提供有关的技术资料和必要的技术指导，帮助委托人掌握研究开发成果。

第八百五十七条 作为技术开发合同标的的技术已经由他人公开，致使技术开发合同的履行没有意义的，当事人可以解除合同。

第八百五十九条 委托开发完成的发明创造，除法律另有规定或者当事人另有约定外，申请专利的权利属于研究开发人。研究开发人取得专利权的，委托人可以依法实施该专利。

研究开发人转让专利申请权的，委托人享有以同等条件优先受让的权利。

第八百六十条 合作开发完成的发明创造，申请专利的权利属于合作开发的当事人共有；当事人一方转让其共有的专利申请权的，其他各方享有以同等条件优先受让的权利。但是，当事人另有约定的除外。

合作开发的当事人一方声明放弃其共有的专利申请权的，除当事人另有约定外，可以由另一方单独申请或者由其他各方共同申请。申请人取得专利权的，放弃专利申请权的一方可以免费实施该专利。

合作开发的当事人一方不同意申请专利的，另一方或者其他各方不得申请专利。

第八百六十一条 委托开发或者合作开发完成的技术秘密成果的使用权、转让权以及收益的分配办法，由当事人约定；没有约定或者约定不明确，依据本法第五百一十条的规定仍不能确定的，在没有相同技术方案被授予专利权前，当事人均有使用和转让的权利。但是，委托

开发的研究开发人不得在向委托人交付研究开发成果之前，将研究开发成果转让给第三人。

第八百六十二条　技术转让合同是合法拥有技术的权利人，将现有特定的专利、专利申请、技术秘密的相关权利让与他人所订立的合同。

技术许可合同是合法拥有技术的权利人，将现有特定的专利、技术秘密的相关权利许可他人实施、使用所订立的合同。

技术转让合同和技术许可合同中关于提供实施技术的专用设备、原材料或者提供有关的技术咨询、技术服务的约定，属于合同的组成部分。

第八百六十三条　技术转让合同包括专利权转让、专利申请权转让、技术秘密转让等合同。

技术许可合同包括专利实施许可、技术秘密使用许可等合同。

技术转让合同和技术许可合同应当采用书面形式。

第八百六十四条　技术转让合同和技术许可合同可以约定实施专利或者使用技术秘密的范围，但是不得限制技术竞争和技术发展。

第八百六十五条　专利实施许可合同仅在该专利权的存续期限内有效。专利权有效期限届满或者专利权被宣告无效的，专利权人不得就该专利与他人订立专利实施许可合同。

第八百六十六条　专利实施许可合同的许可人应当按照约定许可被许可人实施专利，交付实施专利有关的技术资料，提供必要的技术指导。

第八百六十七条　专利实施许可合同的被许可人应当按照约定实施专利，不得许可约定以外的第三人实施该专利，并按照约定支付使用费。

第八百六十八条　技术秘密转让合同的让与人和技术秘密使用许可合同的许可人应当按照约定提供技术资料，进行技术指导，保证技术的实用性、可靠性，承担保密义务。

前款规定的保密义务，不限制许可人申请专利，但是当事人另有约定的除外。

第八百六十九条　技术秘密转让合同的受让人和技术秘密使用许可合同的被许可人应当按照约定使用技术，支付转让费、使用费，承担保密义务。

第八百七十条　技术转让合同的让与人和技术许可合同的许可人应当保证自己是所提供的技术的合法拥有者，并保证所提供的技术完整、无误、有效，能够达到约定的目标。

1.1.4 中华人民共和国刑法（2023 年修正）

第二百一十六条　假冒他人专利，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

第二百一十九条　有下列侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：

（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；

（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；

（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。

明知前款所列行为，获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。

本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。

第二百一十九条之一　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，处五年以下有期徒刑，并处或者单处罚金；情节严重的，处五年以上有期徒刑，并处罚金。

1.1.5 中华人民共和国劳动法（2018 年修正）

第一百零二条 劳动者违反本法规定的条件解除劳动合同或者违反劳动合同中约定的保密事项，对用人单位造成经济损失的，应当依法承担赔偿责任。

1.1.6 中华人民共和国劳动合同法（2012 年修正）

第二十三条 用人单位与劳动者可以在劳动合同中约定保守用人单位的商业秘密和与知识产权相关的保密事项。

对负有保密义务的劳动者，用人单位可以在劳动合同或者保密协议中与劳动者约定竞业限制条款，并约定在解除或者终止劳动合同后，在竞业限制期限内按月给予劳动者经济补偿。劳动者违反竞业限制约定的，应当按照约定向用人单位支付违约金。

1.1.7 中华人民共和国公司法（2023 年修订）

第四十八条 股东可以用货币出资，也可以用实物、知识产权、土地使用权、股权、债权等可以用货币估价并可以依法转让的非货币财产作价出资；但是，法律、行政法规规定不得作为出资的财产除外。

对作为出资的非货币财产应当评估作价，核实财产，不得高估或者低估作价。法律、行政法规对评估作价有规定的，从其规定。

第一百八十一条 董事、监事、高级管理人员不得有下列行为：

……

（五）擅自披露公司秘密

……

1.1.8 天津市知识产权保护条例

（2019 年 9 月 27 日天津市第十七届人民代表大会常务委员会第十三次会议通过）

第一章 总则

第一条 为了加强知识产权保护，激发创新活力，营造尊重知识价值、公平竞争的营商环境，根据有关法律、行政法规的规定，结合本市实际情况，制定本条例。

第二条 本条例适用于本市行政区域内知识产权保护、管理及相关活动。

本条例所称知识产权，是指权利人依法就下列客体享有的专有的权利：

（一）作品；

（二）发明、实用新型、外观设计；

（三）商标；

（四）地理标志；

（五）商业秘密；

（六）集成电路布图设计；

（七）植物新品种；

（八）法律规定的其他客体。

第三条 本市知识产权保护应当遵循全面保护、严格保护、平等保护、依法保护的原则，坚持司法保护、行政保护与社会参与相结合，依法制止不正当竞争行为，维护知识产权权利人和相关权利人的合法权益。

第四条 市和区人民政府应当将知识产权保护工作纳入国民经济和社会发展规划及年度计划，将知识产权保护经费纳入本级财政预算，建立知识产权保护协调机制，统筹推进知识产权保护工作，协调解决知识产权保护工作中的重大问题。

第五条 市和区知识产权部门是本行政区域内知识产权工作的主管部门，负责组织推动知识产权保护、管理等工作，并按照法律、法规的规定履行职权范围内的知识产权保护职责。市场监督管理、规划和自然资源、农业农村、文化和旅游、版权等部门（以下统称知识产权管理部门），按照法律、法规的规定履行各自职权范围内的知识产权保护职责。

第六条 市人民政府应当每年发布知识产权保护白皮书，向社会公示本市知识产权保护状况。市和区人民政府及有关部门应当加强知识产权保护的宣传普及，增强全社会知识产权保护意识和保护能力，营造尊重知识价值、崇尚创新、诚信守法的知识产权保护环境。

鼓励新闻媒体通过多种形式开展知识产权保护的公益宣传。

第七条 自然人、法人和非法人组织应当自觉增强知识产权保护意识和自律意识，提高自我保护能力，抵制知识产权违法行为。

第八条 支持中国（天津）自由贸易试验区和天津经济技术开发区、天津港保税区、天津滨海高新技术产业开发区等国家级开发区依照国家授权，在知识产权保护的体制机制、政策措施、公共服务、信用评价等方面进行探索创新。

第九条 加强京津冀知识产权协同保护，完善案件受理移送、联合调查等工作机制，协调配合跨区域联动查处假冒、侵权案件。

支持京津冀企业、科研机构、高等学校等开展知识产权保护互助与协作，推进知识产权服务资源共享，促进知识产权保护与产业发展深度融合。

第二章 行政保护

第十条 知识产权主管部门依法受理专利、商标、地理标志产品保护的申请，依申请调解、裁决相关纠纷。

市场监督管理部门依法查处假冒专利、商标、地理标志产品的行为，依法查处侵犯专利、商标、地理标志产品等知识产权的行为，依法查处侵犯商业秘密的不正当竞争行为。

规划和自然资源、农业农村部门依法查处假冒授权植物新品种的行为，依法查处侵犯植物新品种权的行为，依申请调解相关纠纷。

版权部门依申请调解著作权纠纷。

文化和旅游部门依法查处侵犯著作权同时损害公共利益的行为。

第十一条 市知识产权主管部门应当制定知识产权分析评议工作指南，加强对知识产权分析评议工作的指导。

发展改革、科技、工业和信息化等部门在重大经济、科技活动中，对可能存在知识产权风险的重大产业规划、重大政府投资项目、重大科技创新项目，按照国家和本市的有关规定，会同知识产权主管部门进行知识产权分析评议，防范知识产权风险。

第十二条 市知识产权主管部门应当按照国家有关规定，为人工智能、生物医药、航空航天、高端装备制造、新能源、新材料等方面的专利申请提供优先审查通道，推动战略性新兴产业

发展。

第十三条 知识产权主管部门和知识产权管理部门应当采取措施，支持文化传承、文化产业、新型文化业态等方面知识产权的创造和保护，引导自然人、法人和非法人组织通过著作权登记、商标注册、商业秘密保护、专利申请等方式维护自身合法权益，推动文化产业创新发展。

第十四条 知识产权主管部门和知识产权管理部门应当鼓励、引导自然人、法人和非法人组织通过著作权登记等方式，保护计算机软件著作权，促进软件产业和信息化发展。

第十五条 市场监督管理部门应当加强商业秘密保护的普法宣传，引导经营者以及其他自然人、法人和非法人组织增强商业秘密管理意识，合理选择保护方式，防止商业秘密泄露。

第十六条 知识产权主管部门和知识产权管理部门应当鼓励、引导自然人、法人和非法人组织将其老字号进行商标注册、域名注册或者专利申请。

第十七条 知识产权主管部门和知识产权管理部门应当鼓励、引导自然人、法人和非法人组织通过申请注册集体商标、证明商标以及申请地理标志产品等方式，加强对地理标志的保护，培育知名度高的地理标志产品集群。

第十八条 规划和自然资源、农业农村部门应当鼓励、引导企业、科研机构、高等学校等申请植物新品种权，促进现代高效农业发展。

规划和自然资源、农业农村、科技部门应当按照国家统筹需要建设植物新品种测试体系，鼓励和支持企业建立种业基地，加强产学研创新协作，促进植物新品种转化与推广。

第十九条 知识产权主管部门和知识产权管理部门应当组织开展知识产权保护的宣传普及，适时发布知识产权保护重要情况通报，支持举办有关知识产权的展览、竞赛、培训、咨询等活动，营造良好知识产权文化氛围。

第二十条 知识产权主管部门应当建立知识产权维权援助机制，受理维权援助申请，提供维权咨询、纠纷解决方案等服务。

第二十一条 知识产权主管部门和知识产权管理部门可以选聘专家作为技术调查员，参与知识产权案件调查，为知识产权行政保护工作提供专业技术支持。

技术调查员根据指派从事下列技术调查工作：

（一）参与调查取证；

（二）对技术事实的调查范围、顺序、方法提出意见；

（三）提出技术审查意见；

（四）知识产权主管部门和知识产权管理部门指派的其他技术调查工作。

市知识产权主管部门和市知识产权管理部门建立知识产权保护专家库，技术调查员应当从专家库中选聘。

第二十二条 知识产权主管部门和知识产权管理部门应当建立统一的投诉、举报平台，公开投诉、举报方式等信息，及时处理并答复收到的投诉、举报。

第三章 社会保护

第二十三条 自然人、法人和非法人组织应当采取措施加强对自身知识产权的保护。

自然人、法人和非法人组织应当尊重他人的知识产权。

自然人、法人和非法人组织可以向有关部门投诉、举报知识产权违法行为，提供相关线索。

第二十四条 企业、科研机构、高等学校建立健全知识产权管理和保护制度，实施知识产权管理国家标准，提升知识产权创造、运用、保护能力，依法维护自身合法权益。

企业、科研机构、高等学校以及其他从事科研活动的单位依法完善分配机制，保障完成职务发明创造、职务育种、职务作品等相关人员的合法权益。

第二十五条 商业秘密权利人建立健全商业秘密管理制度，可以通过给予福利待遇、签订竞

业禁止协议、保密协议等多种方式，对掌握核心商业秘密的相关人员进行激励和约束，提高维护自身权益的能力。

第二十六条 行业组织应当加强对行业内知识产权保护工作的引导，加强对国际国内知识产权状况、发展趋势和竞争态势的监测和研究，加强对成员处理国际、国内知识产权纠纷的信息咨询、维权支持、专业援助等服务。

行业组织应当加强对行业内知识产权保护工作的监督，制定行业知识产权保护自律公约，规范成员创造、运用、保护知识产权的行为。

第二十七条 电子商务经营者应当建立便捷、有效的投诉、举报渠道，公开投诉、举报方式。电子商务平台经营者应当建立知识产权内部监管机制，收到投诉、举报后，应当依法采取必要措施防止侵权损害扩大；知道或者应当知道平台内经营者侵犯知识产权的，应当采取删除、屏蔽、断开链接、终止交易和服务等必要措施。

第二十八条 在本市举办展会，主办方应当在展会举办期间依法保护参展方的知识产权。参展产品、作品、技术或者宣传材料上标注知识产权信息的，参展方应当提供合法有效的知识产权证明文件，未能如实提供的，主办方可以取消其参展资格。

第二十九条 国际性、全国性的体育、文化等重要活动的主办方，应当在知识产权主管部门和知识产权管理部门的指导下，依法规范活动中的知识产权使用行为。未经权利人许可，自然人、法人和非法人组织不得以商业目的使用权利人的知识产权。

第三十条 鼓励高等学校设置知识产权相关专业或者开设知识产权课程，与企业、科研机构、知识产权服务机构合作培养、培训知识产权事业发展所需人才。

企业、科研机构、高等学校以及其他从事科研活动的单位应当注重利用知识产权信息发现人才，加强高层次人才引进、使用中的知识产权评价工作。

第三十一条 鼓励知识产权服务业发展，规范知识产权服务，维护公平竞争的市场秩序，提升知识产权服务水平。

知识产权服务机构依法开展知识产权代理、法律、信息、商用化、咨询、培训等执业活动，不得有下列行为：

（一）泄露委托人商业秘密；

（二）以诋毁其他服务机构等不正当手段招揽业务；

（三）就同一事项接受利害关系人双方委托；

（四）其他损害委托人合法权益的行为。

第三十二条 当事人可以采取公证的方式保管知识产权相关证明材料，为证明知识产权在先使用、公开在先等提供证据支持。

鼓励公证机构创新公证证明方式，优化服务知识产权保护的公证流程，依托电子签名、数据加密等技术为申请人提供远程公证服务。

第三十三条 鼓励、支持知识产权志愿者开展知识产权保护宣传、咨询活动，参与知识产权的网络舆情调查、分析等志愿服务。

第四章 纠纷解决机制

第三十四条 本市建立和完善知识产权纠纷多元解决机制，促进知识产权行政裁决、调解、仲裁、诉讼等纠纷解决途径的有效衔接，保护当事人合法权益，维护公平竞争的市场秩序。

第三十五条 知识产权主管部门依当事人请求，依法对知识产权纠纷作出行政裁决，当事人对行政裁决不服的，可以依法提起诉讼。

知识产权主管部门对知识产权纠纷作出行政裁决前，应当先行调解，调解不成的，应当及时作出行政裁决。

第三十六条 知识产权主管部门和知识产权管理部门依当事人请求，依法对知识产权纠纷进

行调解，调解不成的，当事人可以依法提起民事诉讼。

第三十七条 鼓励人民调解组织、行业协会以及其他社会组织建立知识产权纠纷调解机制。知识产权主管部门和知识产权管理部门、司法行政部门应当根据工作职责，指导人民调解组织、行业协会以及其他社会组织开展知识产权纠纷调解，公平、高效处理知识产权纠纷。

第五章 执法与处罚

第三十八条 知识产权主管部门和知识产权管理部门调查知识产权案件，依法行使下列职权：

（一）采用测量、拍照、摄像等方式对涉嫌违法行为的场所实施现场检查和勘查；

（二）查阅、复制当事人与涉嫌违法行为有关的经营记录、票据、财务账册、合同等资料；

（三）询问当事人，要求其说明有关情况或者提供与被调查行为有关的其他资料；

（四）对证据可能灭失或者以后难以取得的，依法先行登记保存；

（五）依法查封、扣押有证据证明是假冒、侵权的产品、物品；

（六）涉嫌侵犯制造方法专利权等知识产权的，要求当事人进行现场演示，但是应当采取保护措施，防止泄密，并固定相关证据；

（七）法律、法规规定的其他职权。

第三十九条 知识产权主管部门和知识产权管理部门处理知识产权违法案件，涉及违法经营额的，按照下列方法计算：

（一）已销售的违法商品，按照实际销售价格计算；无法查清其实际销售价格的，按照市场在销售的与侵权商品相同或者相似的同类商品的市场中间价格确定。

（二）未销售的违法商品，按照标示价格计算；没有标示价格的，按照市场在销售的与违法商品相同或者相似的同类商品的市场中间价格确定。

（三）法律、法规规定的其他能够合理计算违法商品价格的方法。

查处知识产权案件，发现侵权人多次实施知识产权违法行为且未经行政处理的，其违法经营额应当累计计算。

第四十条 知识产权主管部门和知识产权管理部门依法处理知识产权侵权纠纷，对在本行政区域内侵犯同一知识产权的案件可以依法合并处理；对跨区侵犯同一知识产权的案件可以依法请求市知识产权主管部门和市知识产权管理部门处理。

第四十一条 市场监督管理部门应当依法查处制售假冒伪劣产品和知识产权虚假宣传等行为。发现重大违法线索的，应当对生产、销售等各个环节进行全面调查处理。

第四十二条 网信、版权、公安、文化和旅游等部门应当加强对网络环境的监督，依法查处网络文学、音乐、影视、动漫、游戏、计算机软件等领域的著作权侵权行为。

第四十三条 知识产权主管部门和知识产权管理部门在行政执法过程中或者受理投诉、举报时，发现知识产权违法线索的，应当及时处理；涉嫌犯罪的，应当依法移送公安机关，同时抄送同级检察机关。

第四十四条 市场监督管理部门依专利权人或者利害关系人请求，对经认定的专利侵权行为，责令侵权人立即停止侵权行为。

假冒专利的，由市场监督管理部门责令改正并予以公告，没收违法所得，并处违法所得二倍以上四倍以下的罚款；没有违法所得的，处五万元以上二十万元以下的罚款。

第四十五条 市场监督管理部门依商标权利人或者利害关系人请求，对经认定的商标侵权行为，责令侵权人立即停止侵权行为，没收、销毁侵权商品和主要用于制造侵权商品、伪造注册商标标识的工具，违法经营额五万元以上的，处违法经营额三倍以上五倍以下的罚款；没有违法经营额或者违法经营额不足五万元的，处十万元以上二十五万元以下的罚款。

将未注册商标冒充注册商标使用的，由市场监督管理部门予以制止，限期改正，并予以

通报，违法经营额五万元以上的，处违法经营额百分之二十以下的罚款；没有违法经营额或者违法经营额不足五万元的，处一万元以下的罚款。

第四十六条 侵犯著作权同时损害社会公共利益的，由文化和旅游部门责令停止侵权行为，没收违法所得，没收、销毁侵权复制品，违法经营额五万元以上的，处违法经营额三倍以上五倍以下的罚款；没有违法经营额或者违法经营额不足五万元的，处五万元以上二十五万元以下的罚款；情节严重的，没收主要用于制作侵权复制品的材料、工具、设备等。

第四十七条 侵犯计算机软件著作权同时损害社会公共利益的，由文化和旅游部门依照有关法律、行政法规进行查处。

第四十八条 规划和自然资源、农业农村部门依植物新品种权利人或者利害关系人请求，对经认定的植物新品种侵权行为，涉及社会公共利益的，责令侵权人停止侵权行为，没收违法所得和种子，货值金额五万元以上的，并处货值金额五倍以上十倍以下的罚款；货值金额不足五万元的，并处五万元以上二十五万元以下的罚款。

假冒授权品种的，由规划和自然资源、农业农村部门责令停止违法行为，没收违法所得和种子，货值金额五万元以上的，并处货值金额五倍以上十倍以下的罚款；货值金额不足五万元的，并处五万元以上二十五万元以下的罚款。

第四十九条 侵犯商业秘密的，由市场监督管理部门责令停止违法行为，没收违法所得，处三十万元以上一百万元以下的罚款；情节严重的，处一百万元以上五百万元以下的罚款。法律、行政法规规定由其他部门查处的，依照其规定。

第五十条 将他人注册商标、未注册的驰名商标作为企业名称中的字号使用，误导公众，构成不正当竞争的，由市场监督管理部门责令停止违法行为，没收违法商品，违法经营额五万元以上的，并处违法经营额二倍以上五倍以下的罚款；没有违法经营额或者违法经营额不足五万元的，并处五万元以上二十五万元以下的罚款；情节严重的，吊销营业执照。

第五十一条 自然人、法人和非法人组织因知识产权违法行为受到行政处罚后，五年内重复实施同类违法行为的，知识产权管理部门应当对其依法从重处罚。

第五十二条 拒绝、阻挠知识产权主管部门和知识产权管理部门依法行使职权的，由知识产权主管部门和知识产权管理部门予以警告；构成违反治安管理行为的，由公安机关依法予以治安处罚；构成犯罪的，依法追究刑事责任。

第五十三条 自然人、法人和非法人组织受到知识产权行政处罚，或者拒不执行人民法院已经生效的知识产权判决、裁定和决定，知识产权主管部门和知识产权管理部门、人民法院应当按照国家和本市的有关规定将有关信息纳入统一的信用信息系统。

第五十四条 自然人、法人和非法人组织有知识产权严重失信行为的，有关部门和单位自其发生严重失信行为之日起三年内，按照国家和本市有关规定采取下列联合惩戒措施：

（一）禁止或者限制其承接政府投资项目、参加政府采购和招标投标；

（二）禁止或者限制其享受有关费用减免、政府资金扶持等优惠政策；

（三）取消其进入知识产权快速授权、快速维权通道资格；

（四）取消其参加政府知识产权表彰、奖励的评比资格；

（五）国家和本市规定的其他惩戒措施。

第五十五条 实施知识产权违法行为，依法承担相应民事责任；构成犯罪的，依法追究刑事责任。

实施知识产权违法行为，本条例未作处罚规定的，依照有关法律、法规执行。

第五十六条 技术调查员有下列行为之一的，由聘用的知识产权主管部门和知识产权管理部门予以解聘，并从专家库中除名；给当事人造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

（一）泄露在知识产权案件调查过程中知悉的应予以保密的涉案信息的；

（二）与当事人串通，影响调查取证或者提供不实技术审查意见的；

（三）其他妨碍案件公正处理的行为。

第五十七条 知识产权主管部门和知识产权管理部门及其工作人员怠于履行职责或者滥用职权、玩忽职守、徇私舞弊的，对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

第六章 附则

第五十八条 本条例自 2019 年 11 月 1 日起施行。本条例施行前本市有关地方性法规、政府规章与本条例规定不一致的，按照本条例执行。

1.1.9 浙江省技术秘密保护办法（2008 年修订）

（2005 年 9 月 30 日浙江省人民政府令第 198 号发布　根据 2008 年 7 月 8 日浙江省人民政府令第 246 号公布的《浙江省人民政府关于修改〈浙江省雷电灾害防御和应急办法〉等 3 件规章的决定》修订）

第一条　为了加强对技术秘密权利人（以下简称权利人）正当权益的保护，促进科技进步，根据《中华人民共和国科学技术进步法》、《中华人民共和国反不正当竞争法》及其他有关法律、法规，结合本省实际，制定本办法。

第二条　本办法所称的技术秘密，是指能为权利人带来利益、权利人已采取严格的保密措施、不为公众所知悉的技术信息，包括设计、程序、配方、工艺、方法、诀窍及其他形式的技术信息，属于商业秘密。

第三条　本省行政区域内权利人合法拥有的技术秘密保护适用本办法。属于国家秘密的技术秘密，按照有关法律、法规的规定执行。

第四条　违反法律、法规，损害国家利益、社会公共利益，违背公共道德的技术秘密，不受本办法保护。

第五条　省人民政府科技行政管理部门负责本办法的组织实施；市、县（市、区）人民政府科技行政管理部门负责本行政区域内技术秘密保护的管理和指导。

第六条　县级以上人民政府工商行政管理部门、公安机关按照各自职责查处侵犯技术秘密的行为。

第七条　科技行政管理部门应当加强对权利人技术秘密保护的指导，通过组织培训、技术咨询、制度规范等方式，提高权利人技术秘密保护的意识、能力、水平。

鼓励权利人通过申请专利权保护其技术成果。

第八条　权利人根据技术秘密的特点，建立、健全技术秘密保护的管理制度，配备专职或者兼职的管理人员，对技术秘密保护进行规范化管理。

权利人可以自行选择合法的保护措施、手段和方法，自行确定技术秘密的密级和保护期限，但法律、法规另有规定的，从其规定。

第九条　权利人要求本单位或者与本单位合作的涉及技术秘密的相关人员（以下简称相关人员）保守技术秘密的，应当签订保密协议或者在劳动（聘用）合同（以下统称合同）中作出明确具体的约定。相关人员应当严格按照保密协议或者合同约定履行义务。没有签订保密协议或者没有在合同中作出约定的，相关人员不承担保密责任。保密协议或者合同约定的部分内容不明确的，相关人员只对约定明确的内容承担保密义务。

签订保密协议或者合同约定的相关人员，合同终止后仍负保密义务的，应当书面约定，双方可以就是否支付保密费及其数额进行协商。

第十条　保密协议或者合同约定应当明确下列主要内容：

（一）保密的对象和范围；

（二）双方的权利和义务；

（三）保密期限；

（四）违约责任；

（五）其他需要约定的事项。

第十一条　有下列情形之一的，保密协议或者合同约定自行终止：

（一）约定的保密期限届满的；

（二）该技术秘密已公开的；

（三）权利人不按保密协议或者合同约定支付保密费的。

第十二条　权利人与知悉技术秘密的相关人员可以签订竞业限制协议。

相关人员应当严格按照竞业限制协议约定履行义务。竞业限制协议约定的部分内容不明确的，相关人员只对约定明确的内容承担保密义务。

权利人应当按竞业限制协议约定向履约的相关人员支付一定数额的补偿费。

第十三条　竞业限制协议应当具备以下主要条款：

（一）竞业限制的具体范围；

（二）竞业限制的期限；

（三）补偿费的数额及支付方法；

（四）违约责任；

（五）其他需要约定的事项。

第十四条　竞业限制协议约定的竞业限制期限最长不得超过 2 年；没有约定期限的，竞业限制期限为 2 年。

第十五条　竞业限制补偿费的标准由权利人与相关人员协商确定。没有确定的，年度补偿费按合同终止前最后一个年度该相关人员从权利人处所获得报酬总额的三分之二计算。

第十六条　有下列情形之一的，竞业限制协议终止：

（一）竞业限制期限届满的；

（二）该技术秘密已经公开的；

（三）依法或者协议双方约定终止的其他情形。

协议双方可以约定，权利人违反协议约定不支付或者无正当理由拖欠补偿费，或者权利人违法、违约解除与相关人员合同的，竞业限制协议自行终止。

第十七条　禁止下列侵犯技术秘密行为：

（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的技术秘密；

（二）披露、使用或者允许他人使用以本条第（一）项手段获取的技术秘密；

（三）违反技术秘密保密协议、合同约定或者竞业限制协议，披露、使用或者允许他人使用其所掌握的技术秘密；

（四）获取、使用或者披露明知因本条第（一）、第（二）或者第（三）项所列违法行为而获取或者披露的他人的技术秘密。

第十八条　侵犯权利人技术秘密，造成损害的，应当赔偿损失，并依法承担其他民事责任。

第十九条　当事人对技术秘密损害赔偿额有约定的，按照约定赔偿；没有约定的，可以协商确定；协商不成的，被侵权人可以按下列方式之一计算赔偿额：

（一）按因被侵权所受到的实际损失计算；

（二）按侵权人获取的非法所得及被侵权人进行的相关法律行为所支出的费用的总和计

算。

因侵害行为造成技术秘密完全公开的，应当按该技术秘密的全部价值量赔偿。技术秘密的全部价值量，由具有相应资质的无形资产评估机构评定。

第二十条　违反本办法第十七条规定，侵犯权利人技术秘密的，工商行政管理部门应当责令行为人停止违法行为、返还权利人载有技术秘密的有关资料、停止销售使用权利人技术秘密生产的产品，并按照《中华人民共和国反不正当竞争法》有关规定处以罚款。

国家机关公务人员违反本办法第十七条规定，侵犯权利人技术秘密的，除按照前款规定处罚外，还应当依法给予行政处分。

第二十一条　侵犯技术秘密，构成犯罪的，依法追究刑事责任。

第二十二条　技术秘密的内容在国内外传播媒介上披露，或者在国内被公开使用的，视为该技术秘密已经公开。

第二十三条　本办法自 2006 年 1 月 1 日起施行。

1.2 司法解释

1.2.1 最高人民法院关于适用《中华人民共和国反不正当竞争法》若干问题的解释

（2022 年 1 月 29 日最高人民法院审判委员会第 1862 次会议通过，自 2022 年 3 月 20 日起施行）

为正确审理因不正当竞争行为引发的民事案件，根据《中华人民共和国民法典》《中华人民共和国反不正当竞争法》《中华人民共和国民事诉讼法》等有关法律规定，结合审判实践，制定本解释。

第一条　经营者扰乱市场竞争秩序，损害其他经营者或者消费者合法权益，且属于违反反不正当竞争法第二章及专利法、商标法、著作权法等规定之外情形的，人民法院可以适用反不正当竞争法第二条予以认定。

第二条　与经营者在生产经营活动中存在可能的争夺交易机会、损害竞争优势等关系的市场主体，人民法院可以认定为反不正当竞争法第二条规定的“其他经营者”。

第三条　特定商业领域普遍遵循和认可的行为规范，人民法院可以认定为反不正当竞争法第二条规定的“商业道德”。

人民法院应当结合案件具体情况，综合考虑行业规则或者商业惯例、经营者的主观状态、交易相对人的选择意愿、对消费者权益、市场竞争秩序、社会公共利益的影响等因素，依法判断经营者是否违反商业道德。

人民法院认定经营者是否违反商业道德时，可以参考行业主管部门、行业协会或者自律组织制定的从业规范、技术规范、自律公约等。

第四条　具有一定的市场知名度并具有区别商品来源的显著特征的标识，人民法院可以认定为反不正当竞争法第六条规定的“有一定影响的”标识。

人民法院认定反不正当竞争法第六条规定的标识是否具有一定的市场知名度，应当综合考虑中国境内相关公众的知悉程度，商品销售的时间、区域、数额和对象，宣传的持续时间、程度和地域范围，标识受保护的情况等因素。

第五条　反不正当竞争法第六条规定的标识有下列情形之一的，人民法院应当认定其不具有区别商品来源的显著特征：

（一）商品的通用名称、图形、型号；

（二）仅直接表示商品的质量、主要原料、功能、用途、重量、数量及其他特点的标识；

（三）仅由商品自身的性质产生的形状，为获得技术效果而需有的商品形状以及使商品具有实质性价值的形状；

（四）其他缺乏显著特征的标识。

前款第一项、第二项、第四项规定的标识经过使用取得显著特征，并具有一定的市场知名度，当事人请求依据反不正当竞争法第六条规定予以保护的，人民法院应予支持。

第六条　因客观描述、说明商品而正当使用下列标识，当事人主张属于反不正当竞争法第六条规定的情形的，人民法院不予支持：

（一）含有本商品的通用名称、图形、型号；

（二）直接表示商品的质量、主要原料、功能、用途、重量、数量以及其他特点；

（三）含有地名。

第七条　反不正当竞争法第六条规定的标识或者其显著识别部分属于商标法第十条第一款规定的不得作为商标使用的标志，当事人请求依据反不正当竞争法第六条规定予以保护的，人民法院不予支持。

第八条　由经营者营业场所的装饰、营业用具的式样、营业人员的服饰等构成的具有独特风格的整体营业形象，人民法院可以认定为反不正当竞争法第六条第一项规定的“装潢”。

第九条　市场主体登记管理部门依法登记的企业名称，以及在中国境内进行商业使用的境外企业名称，人民法院可以认定为反不正当竞争法第六条第二项规定的“企业名称”。

有一定影响的个体工商户、农民专业合作社（联合社）以及法律、行政法规规定的其他市场主体的名称（包括简称、字号等），人民法院可以依照反不正当竞争法第六条第二项予以认定。

第十条　在中国境内将有一定影响的标识用于商品、商品包装或者容器以及商品交易文书上，或者广告宣传、展览以及其他商业活动中，用于识别商品来源的行为，人民法院可以认定为反不正当竞争法第六条规定的“使用”。

第十一条　经营者擅自使用与他人有一定影响的企业名称（包括简称、字号等）、社会组织名称（包括简称等）、姓名（包括笔名、艺名、译名等）、域名主体部分、网站名称、网页等近似的标识，引人误认为是他人商品或者与他人存在特定联系，当事人主张属于反不正当竞争法第六条第二项、第三项规定的情形的，人民法院应予支持。

第十二条　人民法院认定与反不正当竞争法第六条规定的“有一定影响的”标识相同或者近似，可以参照商标相同或者近似的判断原则和方法。

反不正当竞争法第六条规定的“引人误认为是他人商品或者与他人存在特定联系”，包括误认为与他人具有商业联合、许可使用、商业冠名、广告代言等特定联系。

在相同商品上使用相同或者视觉上基本无差别的商品名称、包装、装潢等标识，应当视为足以造成与他人有一定影响的标识相混淆。

第十三条　经营者实施下列混淆行为之一，足以引人误认为是他人商品或者与他人存在特定联系的，人民法院可以依照反不正当竞争法第六条第四项予以认定：

（一）擅自使用反不正当竞争法第六条第一项、第二项、第三项规定以外“有一定影响的”标识；

（二）将他人注册商标、未注册的驰名商标作为企业名称中的字号使用，误导公众。

第十四条　经营者销售带有违反反不正当竞争法第六条规定的标识的商品，引人误认为是他人商品或者与他人存在特定联系，当事人主张构成反不正当竞争法第六条规定的情形的，人民法院应予支持。

销售不知道是前款规定的侵权商品，能证明该商品是自己合法取得并说明提供者，经营

者主张不承担赔偿责任的，人民法院应予支持。

第十五条　故意为他人实施混淆行为提供仓储、运输、邮寄、印制、隐匿、经营场所等便利条件，当事人请求依据民法典第一千一百六十九条第一款予以认定的，人民法院应予支持。

第十六条　经营者在商业宣传过程中，提供不真实的商品相关信息，欺骗、误导相关公众的，人民法院应当认定为反不正当竞争法第八条第一款规定的虚假的商业宣传。

第十七条　经营者具有下列行为之一，欺骗、误导相关公众的，人民法院可以认定为反不正当竞争法第八条第一款规定的“引人误解的商业宣传”：

（一）对商品作片面的宣传或者对比；

（二）将科学上未定论的观点、现象等当作定论的事实用于商品宣传；

（三）使用歧义性语言进行商业宣传；

（四）其他足以引人误解的商业宣传行为。

人民法院应当根据日常生活经验、相关公众一般注意力、发生误解的事实和被宣传对象的实际情况等因素，对引人误解的商业宣传行为进行认定。

第十八条　当事人主张经营者违反反不正当竞争法第八条第一款的规定并请求赔偿损失的，应当举证证明其因虚假或者引人误解的商业宣传行为受到损失。

第十九条　当事人主张经营者实施了反不正当竞争法第十一条规定的商业诋毁行为的，应当举证证明其为该商业诋毁行为的特定损害对象。

第二十条　经营者传播他人编造的虚假信息或者误导性信息，损害竞争对手的商业信誉、商品声誉的，人民法院应当依照反不正当竞争法第十一条予以认定。

第二十一条　未经其他经营者和用户同意而直接发生的目标跳转，人民法院应当认定为反不正当竞争法第十二条第二款第一项规定的“强制进行目标跳转”。

仅插入链接，目标跳转由用户触发的，人民法院应当综合考虑插入链接的具体方式、是否具有合理理由以及对用户利益和其他经营者利益的影响等因素，认定该行为是否违反反不正当竞争法第十二条第二款第一项的规定。

第二十二条　经营者事前未明确提示并经用户同意，以误导、欺骗、强迫用户修改、关闭、卸载等方式，恶意干扰或者破坏其他经营者合法提供的网络产品或者服务，人民法院应当依照反不正当竞争法第十二条第二款第二项予以认定。

第二十三条　对于反不正当竞争法第二条、第八条、第十一条、第十二条规定的不正当竞争行为，权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益难以确定，当事人主张依据反不正当竞争法第十七条第四款确定赔偿数额的，人民法院应予支持。

第二十四条　对于同一侵权人针对同一主体在同一时间和地域范围实施的侵权行为，人民法院已经认定侵害著作权、专利权或者注册商标专用权等并判令承担民事责任，当事人又以该行为构成不正当竞争为由请求同一侵权人承担民事责任的，人民法院不予支持。

第二十五条　依据反不正当竞争法第六条的规定，当事人主张判令被告停止使用或者变更其企业名称的诉讼请求依法应予支持的，人民法院应当判令停止使用该企业名称。

第二十六条　因不正当竞争行为提起的民事诉讼，由侵权行为地或者被告住所地人民法院管辖。

当事人主张仅以网络购买者可以任意选择的收货地作为侵权行为地的，人民法院不予支持。

第二十七条　被诉不正当竞争行为发生在中华人民共和国领域外，但侵权结果发生在中华人民共和国领域内，当事人主张由该侵权结果发生地人民法院管辖的，人民法院应予支持。

第二十八条　反不正当竞争法修改决定施行以后人民法院受理的不正当竞争民事案件，涉及该决定施行前发生的行为的，适用修改前的反不正当竞争法；涉及该决定施行前发生、持续到该决定施行以后的行为的，适用修改后的反不正当竞争法。

第二十九条　本解释自 2022 年 3 月 20 日起施行。《最高人民法院关于审理不正当竞争民事案件应用法律若干问题的解释》（法释〔2007〕2 号）同时废止。

本解释施行以后尚未终审的案件，适用本解释；施行以前已经终审的案件，不适用本解释再审。

1.2.2 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

（2020 年 8 月 24 日最高人民法院审判委员会第 1810 次会议通过，自 2020 年 9 月 12 日起施行）

为正确审理侵犯商业秘密民事案件，根据《中华人民共和国反不正当竞争法》《中华人民共和国民事诉讼法》等有关法律规定，结合审判实际，制定本规定。

第一条 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，人民法院可以认定构成反不正当竞争法第九条第四款所称的技术信息。

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，人民法院可以认定构成反不正当竞争法第九条第四款所称的经营信息。

前款所称的客户信息，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。

第二条 当事人仅以与特定客户保持长期稳定交易关系为由，主张该特定客户属于商业秘密的，人民法院不予支持。

客户基于对员工个人的信赖而与该员工所在单位进行交易，该员工离职后，能够证明客户自愿选择与该员工或者该员工所在的新单位进行交易的，人民法院应当认定该员工没有采用不正当手段获取权利人的商业秘密。

第三条 权利人请求保护的信息在被诉侵权行为发生时不为所属领域的相关人员普遍知悉和容易获得的，人民法院应当认定为反不正当竞争法第九条第四款所称的不为公众所知悉。

第四条 具有下列情形之一的，人民法院可以认定有关信息为公众所知悉：

（一）该信息在所属领域属于一般常识或者行业惯例的；

（二）该信息仅涉及产品的尺寸、结构、材料、部件的简单组合等内容，所属领域的相关人员通过观察上市产品即可直接获得的；

（三）该信息已经在公开出版物或者其他媒体上公开披露的；

（四）该信息已通过公开的报告会、展览等方式公开的；

（五）所属领域的相关人员从其他公开渠道可以获得该信息的。

将为公众所知悉的信息进行整理、改进、加工后形成的新信息，符合本规定第三条规定的，应当认定该新信息不为公众所知悉。

第五条 权利人为防止商业秘密泄露，在被诉侵权行为发生以前所采取的合理保密措施，人民法院应当认定为反不正当竞争法第九条第四款所称的相应保密措施。

人民法院应当根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素，认定权利人是否采取了相应保密措施。

第六条 具有下列情形之一，在正常情况下足以防止商业秘密泄露的，人民法院应当认定权

利人采取了相应保密措施：

（一）签订保密协议或者在合同中约定保密义务的；

（二）通过章程、培训、规章制度、书面告知等方式，对能够接触、获取商业秘密的员工、前员工、供应商、客户、来访者等提出保密要求的；

（三）对涉密的厂房、车间等生产经营场所限制来访者或者进行区分管理的；

（四）以标记、分类、隔离、加密、封存、限制能够接触或者获取的人员范围等方式，对商业秘密及其载体进行区分和管理的；

（五）对能够接触、获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等，采取禁止或者限制使用、访问、存储、复制等措施的；

（六）要求离职员工登记、返还、清除、销毁其接触或者获取的商业秘密及其载体，继续承担保密义务的；

（七）采取其他合理保密措施的。

第七条 权利人请求保护的信息因不为公众所知悉而具有现实的或者潜在的商业价值的，人民法院经审查可以认定为反不正当竞争法第九条第四款所称的具有商业价值。

生产经营活动中形成的阶段性成果符合前款规定的，人民法院经审查可以认定该成果具有商业价值。

第八条 被诉侵权人以违反法律规定或者公认的商业道德的方式获取权利人的商业秘密的，人民法院应当认定属于反不正当竞争法第九条第一款所称的以其他不正当手段获取权利人的商业秘密。

第九条 被诉侵权人在生产经营活动中直接使用商业秘密，或者对商业秘密进行修改、改进后使用，或者根据商业秘密调整、优化、改进有关生产经营活动的，人民法院应当认定属于反不正当竞争法第九条所称的使用商业秘密。

第十条 当事人根据法律规定或者合同约定所承担的保密义务，人民法院应当认定属于反不正当竞争法第九条第一款所称的保密义务。

当事人未在合同中约定保密义务，但根据诚信原则以及合同的性质、目的、缔约过程、交易习惯等，被诉侵权人知道或者应当知道其获取的信息属于权利人的商业秘密的，人民法院应当认定被诉侵权人对其获取的商业秘密承担保密义务。

第十一条 法人、非法人组织的经营、管理人员以及具有劳动关系的其他人员，人民法院可以认定为反不正当竞争法第九条第三款所称的员工、前员工。

第十二条 人民法院认定员工、前员工是否有渠道或者机会获取权利人的商业秘密，可以考虑与其有关的下列因素：

（一）职务、职责、权限；

（二）承担的本职工作或者单位分配的任务；

（三）参与和商业秘密有关的生产经营活动的具体情形；

（四）是否保管、使用、存储、复制、控制或者以其他方式接触、获取商业秘密及其载体；

（五）需要考虑的其他因素。

第十三条 被诉侵权信息与商业秘密不存在实质性区别的，人民法院可以认定被诉侵权信息与商业秘密构成反不正当竞争法第三十二条第二款所称的实质上相同。

人民法院认定是否构成前款所称的实质上相同，可以考虑下列因素：

（一）被诉侵权信息与商业秘密的异同程度；

（二）所属领域的相关人员在被诉侵权行为发生时是否容易想到被诉侵权信息与商业秘密的区别；

（三）被诉侵权信息与商业秘密的用途、使用方式、目的、效果等是否具有实质性差异；

（四）公有领域中与商业秘密相关信息的情况；

（五）需要考虑的其他因素。

第十四条 通过自行开发研制或者反向工程获得被诉侵权信息的，人民法院应当认定不属于反不正当竞争法第九条规定的侵犯商业秘密行为。

前款所称的反向工程，是指通过技术手段对从公开渠道取得的产品进行拆卸、测绘、分析等而获得该产品的有关技术信息。

被诉侵权人以不正当手段获取权利人的商业秘密后，又以反向工程为由主张未侵犯商业秘密的，人民法院不予支持。

第十五条 被申请人试图或者已经以不正当手段获取、披露、使用或者允许他人使用权利人所主张的商业秘密，不采取行为保全措施会使判决难以执行或者造成当事人其他损害，或者将会使权利人的合法权益受到难以弥补的损害的，人民法院可以依法裁定采取行为保全措施。前款规定的情形属于民事诉讼法第一百条、第一百零一条所称情况紧急的，人民法院应当在四十八小时内作出裁定。

第十六条 经营者以外的其他自然人、法人和非法人组织侵犯商业秘密，权利人依据反不正当竞争法第十七条的规定主张侵权人应当承担的民事责任的，人民法院应予支持。

第十七条 人民法院对于侵犯商业秘密行为判决停止侵害的民事责任时，停止侵害的时间一般应当持续到该商业秘密已为公众所知悉时为止。

依照前款规定判决停止侵害的时间明显不合理的，人民法院可以在依法保护权利人的商业秘密竞争优势的情况下，判决侵权人在一定期限或者范围内停止使用该商业秘密。

第十八条 权利人请求判决侵权人返还或者销毁商业秘密载体，清除其控制的商业秘密信息的，人民法院一般应予支持。

第十九条 因侵权行为导致商业秘密为公众所知悉的，人民法院依法确定赔偿数额时，可以考虑商业秘密的商业价值。

人民法院认定前款所称的商业价值，应当考虑研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素。

第二十条 权利人请求参照商业秘密许可使用费确定因被侵权所受到的实际损失的，人民法院可以根据许可的性质、内容、实际履行情况以及侵权行为的性质、情节、后果等因素确定。

人民法院依照反不正当竞争法第十七条第四款确定赔偿数额的，可以考虑商业秘密的性质、商业价值、研究开发成本、创新程度、能带来的竞争优势以及侵权人的主观过错、侵权行为的性质、情节、后果等因素。

第二十一条 对于涉及当事人或者案外人的商业秘密的证据、材料，当事人或者案外人书面申请人民法院采取保密措施的，人民法院应当在保全、证据交换、质证、委托鉴定、询问、庭审等诉讼活动中采取必要的保密措施。

违反前款所称的保密措施的要求，擅自披露商业秘密或者在诉讼活动之外使用或者允许他人使用在诉讼中接触、获取的商业秘密的，应当依法承担民事责任。构成民事诉讼法第一百一十一条规定情形的，人民法院可以依法采取强制措施。构成犯罪的，依法追究刑事责任。

第二十二条 人民法院审理侵犯商业秘密民事案件时，对在侵犯商业秘密犯罪刑事诉讼程序中形成的证据，应当按照法定程序，全面、客观地审查。

由公安机关、检察机关或者人民法院保存的与被诉侵权行为具有关联性的证据，侵犯商业秘密民事案件的当事人及其诉讼代理人因客观原因不能自行收集，申请调查收集的，人民法院应当准许，但可能影响正在进行的刑事诉讼程序的除外。

第二十三条 当事人主张依据生效刑事裁判认定的实际损失或者违法所得确定涉及同一侵犯商业秘密行为的民事案件赔偿数额的，人民法院应予支持。

第二十四条 权利人已经提供侵权人因侵权所获得的利益的初步证据，但与侵犯商业秘密行

为相关的账簿、资料由侵权人掌握的，人民法院可以根据权利人的申请，责令侵权人提供该账簿、资料。侵权人无正当理由拒不提供或者不如实提供的，人民法院可以根据权利人的主张和提供的证据认定侵权人因侵权所获得的利益。

第二十五条 当事人以涉及同一被诉侵犯商业秘密行为的刑事案件尚未审结为由，请求中止审理侵犯商业秘密民事案件，人民法院在听取当事人意见后认为必须以该刑事案件的审理结果为依据的，应予支持。

第二十六条 对于侵犯商业秘密行为，商业秘密独占使用许可合同的被许可人提起诉讼的，人民法院应当依法受理。

排他使用许可合同的被许可人和权利人共同提起诉讼，或者在权利人不起诉的情况下自行提起诉讼的，人民法院应当依法受理。

普通使用许可合同的被许可人和权利人共同提起诉讼，或者经权利人书面授权单独提起诉讼的，人民法院应当依法受理。

第二十七条 权利人应当在一审法庭辩论结束前明确所主张的商业秘密具体内容。仅能明确部分的，人民法院对该明确的部分进行审理。

权利人在第二审程序中另行主张其在一审中未明确的商业秘密具体内容的，第二审人民法院可以根据当事人自愿的原则就与该商业秘密具体内容有关的诉讼请求进行调解；调解不成的，告知当事人另行起诉。双方当事人均同意由第二审人民法院一并审理的，第二审人民法院可以一并裁判。

第二十八条 人民法院审理侵犯商业秘密民事案件，适用被诉侵权行为发生时的法律。被诉侵权行为在法律修改之前已经发生且持续到法律修改之后的，适用修改后的法律。

第二十九条 本规定自 2020 年 9 月 12 日起施行。最高人民法院以前发布的相关司法解释与本规定不一致的，以本规定为准。

本规定施行后，人民法院正在审理的一审、二审案件适用本规定；施行前已经作出生效裁判的案件，不适用本规定再审。

1.2.3 最高人民法院关于适用《中华人民共和国刑事诉讼法》的解释（2021）

第五十五条 查阅、摘抄、复制案卷材料，涉及国家秘密、商业秘密、个人隐私的，应当保密；对不公开审理案件的信息、材料，或者在办案过程中获悉的案件重要信息、证据材料，不得违反规定泄露、披露，不得用于办案以外的用途。人民法院可以要求相关人员出具承诺书。

第八十一条 公开审理案件时，公诉人、诉讼参与人提出涉及国家秘密、商业秘密或者个人隐私的证据的，法庭应当制止；确与本案有关的，可以根据具体情况，决定将案件转为不公开审理，或者对相关证据的法庭调查不公开进行。

第一百三十五条 法庭决定对证据收集的合法性进行调查的，由公诉人通过宣读调查、侦查讯问笔录、出示提讯登记、体检记录、对讯问合法性的核查材料等证据材料，有针对性地播放讯问录音录像，提请法庭通知有关调查人员、侦查人员或者其他人员出庭说明情况等方式，证明证据收集的合法性。

讯问录音录像涉及国家秘密、商业秘密、个人隐私或者其他不宜公开内容的，法庭可以决定对讯问录音录像不公开播放、质证。

第二百二十二条　审判案件应当公开进行。

案件涉及国家秘密或者个人隐私的，不公开审理；涉及商业秘密，当事人提出申请的，法庭可以决定不公开审理。

第二百八十七条　审判长宣布法庭辩论终结后，合议庭应当保证被告人充分行使最后陈述的权利。

被告人在最后陈述中多次重复自己的意见的，法庭可以制止；陈述内容蔑视法庭、公诉人，损害他人及社会公共利益，或者与本案无关的，应当制止。

在公开审理的案件中，被告人最后陈述的内容涉及国家秘密、个人隐私或者商业秘密的，应当制止。

1.2.4 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4月7日最高人民法院审判委员会第1947次会议、2025年4月11日最高人民检察院第十四届检察委员会第五十一次会议通过，自2025年4月26日起施行)

为依法惩治侵犯知识产权犯罪，维护社会主义市场经济秩序，根据《中华人民共和国刑法》《中华人民共和国刑事诉讼法》等法律的有关规定，结合司法实践，现就办理侵犯知识产权刑事案件适用法律的若干问题解释如下：

第十六条 采取非法复制等方式获取商业秘密的，应当认定为刑法第二百一十九条第一款第一项规定的“盗窃”；未经授权或者超越授权使用计算机信息系统等方式获取商业秘密的，应当认定为刑法第二百一十九条第一款第一项规定的“电子侵入”。

第十七条 侵犯商业秘密，具有下列情形之一的，应当认定为刑法第二百一十九条规定的“情节严重”：

(一)给商业秘密的权利人造成损失数额在三十万元以上的；

(二)因侵犯商业秘密违法所得数额在三十万元以上的；

(三)二年内因实施刑法第二百一十九条、第二百一十九条之一规定的行为受过刑事处罚或者行政处罚后再次实施，造成损失数额或者违法所得数额在十万元以上的；

(四)其他情节严重的情形。

侵犯商业秘密，直接导致商业秘密的权利人因重大经营困难而破产、倒闭的，或者数额达到本条前款相应规定标准十倍以上的，应当认定为刑法第二百一十九条规定的“情节特别严重”。

第十八条 本解释规定的侵犯商业秘密“损失数额”，按照下列方式予以认定：

(一)以不正当手段获取权利人的商业秘密，尚未披露、使用或者允许他人使用的，损失数额可以根据该项商业秘密的合理许可使用费确定；

(二)以不正当手段获取权利人的商业秘密后，披露、使用或者允许他人使用的，损失数额可以根据权利人因被侵权造成利润的损失确定，但该损失数额低于商业秘密合理许可使用费的，根据合理许可使用费确定；

(三)违反保密义务或者权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的，损失数额可以根据权利人因被侵权造成利润的损失确定；

(四)明知商业秘密是不正当手段获取或者是违反保密义务、权利人有关保守商业秘密的要求披露、使用、允许使用，仍获取、披露、使用或者允许他人使用的，损失数额可以根据

权利人因被侵权造成利润的损失确定;

(五)因侵犯商业秘密行为导致商业秘密已为公众所知悉或者灭失的，损失数额可以根据该项商业秘密的商业价值确定。商业秘密的商业价值，可以根据该项商业秘密的研究开发成本、实施该项商业秘密的收益等因素综合确定。

前款第二项至第四项规定的权利人因被侵权造成利润的损失,可以根据权利人因被侵权造成产品销售量减少的总数乘以权利人每件产品的合理利润确定;产品销售量减少的总数无法确定的，可以根据侵权产品销售量乘以权利人每件产品的合理利润确定。商业秘密系用于服务等其他经营活动的，损失数额可以根据权利人因被侵权而减少的合理利润确定。

商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用，应当计入给商业秘密的权利人造成的损失。

第十九条 本解释规定的侵犯商业秘密“违法所得数额”，是指因披露、允许他人使用商业秘密而获得的财物或者其他财产性利益的价值，或者因使用商业秘密所获得的利润。该利润可以根据侵权产品销售量乘以每件侵权产品的合理利润确定。

第二十条 为境外机构、组织、人员窃取、刺探、收买、非法提供商业秘密，具有本解释第十七条规定情形的，应当认定为刑法第二百一十九条之一规定的“情节严重”。

第二十一条 在刑事诉讼程序中，当事人、辩护人、诉讼代理人或者案外人书面申请对有关商业秘密或者其他需要保密的商业信息的证据、材料采取保密措施的，应当根据案件情况采取组织诉讼参与人签署保密承诺书等必要的保密措施。

违反前款有关保密措施的要求或者法律法规规定的保密义务的，依法承担相应责任。擅自披露、使用或者允许他人使用在刑事诉讼程序中接触、获取的商业秘密，构成犯罪的，依法追究刑事责任。

第二十四条 实施侵犯知识产权犯罪，具有下列情形之一的，可以依法从轻处罚:

(一)认罪认罚的;

(二)取得权利人谅解的;

(三)以不正当手段获取权利人的商业秘密后尚未披露、使用或者允许他人使用的。

犯罪情节轻微的，可以依法不起诉或者免予刑事处罚。情节显著轻微危害不大的，不以犯罪论处。

第二十五条 实施侵犯知识产权犯罪的，应当综合考虑犯罪违法所得数额、非法经营数额、给权利人造成的损失数额、侵权假冒物品数量及社会危害性等情节，依法判处罚金。

罚金数额一般在违法所得数额的一倍以上十倍以下确定。违法所得数额无法查清的，罚金数额一般按照非法经营数额的百分之五十以上一倍以下确定。违法所得数额和非法经营数额均无法查清，判处三年以下有期徒刑、拘役或者单处罚金的，一般在三万元以上一百万元以下确定罚金数额;判处三年以上有期徒刑的，一般在十五万元以上五百万元以下确定罚金数额。

第二十六条 单位实施刑法第二百一十三条至第二百一十九条之一行为的,对单位判处罚金,并对其直接负责的主管人员和其他直接责任人员，依照本解释规定的定罪量刑标准处罚。

第二十八条 本解释所称“非法经营数额”，是指行为人在实施侵犯知识产权行为过程中，制造、储存、运输、销售侵权产品的价值。已销售侵权产品的价值，按照实际销售的价格计算。尚未销售侵权产品的价值，按照已经查清的侵权产品实际销售平均价格计算。实际销售平均价格无法查清的，按照侵权产品的标价计算。无法查清实际销售价格或者侵权产品没有标价的，按照被侵权产品的市场中间价格计算。

本解释所称“货值金额”，依照前款规定的尚未销售的侵犯知识产权的产品价值认定。本解释所称“销售金额”，是指行为人在实施侵犯知识产权行为过程中，出售侵权产品后所得和应得的全部违法收入。

本解释所称“违法所得数额”，是指行为人出售侵犯知识产权的产品后所得和应得的全部违法收入扣除原材料、所售产品的购进价款;提供服务的，扣除该项服务中所使用产品的购进价款。通过收取服务费、会员费或者广告费等方式营利的，收取的费用应当认定为“违法所得”。

第二十九条 多次实施侵犯知识产权行为，未经处理且依法应当追诉的，定罪量刑所涉数额、数量等分别累计计算。

对于已经制作完成但尚未附着或者尚未全部附着假冒注册商标标识的产品，有证据证明该产品将假冒他人注册商标的，其价值计入非法经营数额。

第三十条 人民法院依法受理侵犯知识产权刑事自诉案件，对于当事人因客观原因不能取得的证据，在提起自诉时能够提供有关线索，申请人民法院调取的，人民法院应当依法调取。

第三十一条 本解释自 2025 年 4 月 26 日起施行。

1.2.5 最高人民检察院、公安部关于印发《关于修改侵犯商业秘密刑事案件立案追诉标准的决定》的通知

为依法惩治侵犯商业秘密犯罪，加大对知识产权的刑事司法保护力度，维护社会主义市场经济秩序，将《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定（二）》第七十三条侵犯商业秘密刑事案件立案追诉标准修改为：【侵犯商业秘密案（刑法第二百一十九条）】 侵犯商业秘密，涉嫌下列情形之一的，应予立案追诉：

（一）给商业秘密权利人造成损失数额在三十万元以上的；

（二）因侵犯商业秘密违法所得数额在三十万元以上的；

（三）直接导致商业秘密的权利人因重大经营困难而破产、倒闭的；

（四）其他给商业秘密权利人造成重大损失的情形。

前款规定的造成损失数额或者违法所得数额，可以按照下列方式认定：

（一）以不正当手段获取权利人的商业秘密，尚未披露、使用或者允许他人使用的，损失数额可以根据该项商业秘密的合理许可使用费确定；

（二）以不正当手段获取权利人的商业秘密后，披露、使用或者允许他人使用的，损失数额可以根据权利人因被侵权造成销售利润的损失确定，但该损失数额低于商业秘密合理许可使用费的，根据合理许可使用费确定；

（三）违反约定、权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的，损失数额可以根据权利人因被侵权造成销售利润的损失确定；

（四）明知商业秘密是不正当手段获取或者是违反约定、权利人有关保守商业秘密的要求披露、使用、允许使用，仍获取、使用或者披露的，损失数额可以根据权利人因被侵权造成销售利润的损失确定；

（五）因侵犯商业秘密行为导致商业秘密已为公众所知悉或者灭失的，损失数额可以根据该项商业秘密的商业价值确定。商业秘密的商业价值，可以根据该项商业秘密的研究开发成本、实施该项商业秘密的收益综合确定；

（六）因披露或者允许他人使用商业秘密而获得的财物或者其他财产性利益，应当认定为违法所得。

前款第二项、第三项、第四项规定的权利人因被侵权造成销售利润的损失，可以根据权利人因被侵权造成销售量减少的总数乘以权利人每件产品的合理利润确定；销售量减少的总数无法确定的，可以根据侵权产品销售量乘以权利人每件产品的合理利润确定；权利人因被

侵权造成销售量减少的总数和每件产品的合理利润均无法确定的，可以根据侵权产品销售量乘以每件侵权产品的合理利润确定。商业秘密系用于服务等其他经营活动的，损失数额可以根据权利人因被侵权而减少的合理利润确定。

商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用，应当计入给商业秘密的权利人造成的损失。

1.3 部门规章

1.3.1 劳动和社会保障部办公厅关于劳动争议案中涉及商业秘密侵权问题的函

（劳社厅函〔1999〕69 号）

河南省劳动厅：

你厅《关于劳动争议案中商业秘密侵权问题的请示》（豫劳函〔1999〕20 号）收悉。经研究，现函复如下：

一、《中华人民共和国反不正当竞争法》第二十条第一款规定了被侵害的经营者的损失难以计算时，确定侵权人的赔偿项目；第二款规定了被侵害的经营者的合法权益受到侵害，可以向人民法院提起诉讼。原劳动部《违反＜劳动法＞有关劳动合同规定的赔偿办法》（劳部发〔1995〕223 号）第五、六条关于按《反不正当竞争法》第二十条规定执行的含义，是指适用第一款的规定。

二、劳动合同中如果明确约定了有关保守商业秘密的内容，由于劳动者未履行，造成用人单位商业秘密被侵害而发生劳动争议，当事人向劳动争议仲裁委员会申请仲裁的，仲裁委员会应当受理，并依据有关规定和劳动合同的约定作出裁决。

1.3.2 国家工商行政管理局关于商业秘密构成要件问题的答复

（工商公字〔1998〕第 109 号）

江苏省工商行政管理局：

你局《关于权利人提供的技术信息能否定为商业秘密的请示》（苏工商〔1998〕41 号）收悉。经研究，答复如下：

商业秘密的构成要件有三：一是该信息不为公众所知悉，即该信息是不能从公开渠道直接获取的；二是该信息能为权利人带来经济利益，具有实用性；三是权利人对该信息采取了保密措施。概括地说，不能从公开渠道直接获取的，能为权利人带来经济利益，具有实用性，并经权利人采取保密措施的信息，即为《反不正当竞争法》所保护的商业秘密。

权利人采取保密措施，包括口头或书面的保密协议、对商业秘密权利人的职工或与商业秘密权利人有业务关系的他人提出保密要求等合理措施。只要权利人提出了保密要求，商业秘密权利人的职工或与商业秘密权利人有业务关系的他人知道或应该知道存在商业秘密，即为权利人采取了合理的保密措施，职工或他人就对权利人承担保密义务。

1.3.3 国务院国有资产监督管理委员会关于印发《中央企业商业秘密保护暂行规定》的通知

各中央企业：

《中央企业商业秘密保护暂行规定》已经国务院国有资产监督管理委员会第87次主任办公会议审议通过，现印发给你们，请遵照执行。

各中央企业要高度重视商业秘密保护工作，加快研究制订相关实施细则，切实保障企业利益不受侵害，促进企业又好又快发展。

1.3.4 国务院国有资产监督管理委员会关于印发《中央企业商业秘密保护暂行规定》的通知

第一章　总则
第一条　为加强中央企业商业秘密保护工作，保障中央企业利益不受侵害，根据《中华人民共和国保守国家秘密法》和《中华人民共和国反不正当竞争法》等法律法规，制定本规定。
第二条　本规定所称的商业秘密，是指不为公众所知悉、能为中央企业带来经济利益、具有实用性并经中央企业采取保密措施的经营信息和技术信息。
第三条　中央企业经营信息和技术信息中属于国家秘密范围的，必须依法按照国家秘密进行保护。
第四条　中央企业商业秘密中涉及知识产权内容的，按国家知识产权有关法律法规进行管理。
第五条　中央企业商业秘密保护工作，实行依法规范、企业负责、预防为主、突出重点、便利工作、保障安全的方针。

第二章　机构与职责
第六条　中央企业商业秘密保护工作按照统一领导、分级管理的原则，实行企业法定代表人负责制。
第七条　各中央企业保密委员会是商业秘密保护工作的工作机构，负责贯彻国家有关法律、法规和规章，落实上级保密机构、部门的工作要求，研究决定企业商业秘密保护工作的相关事项。
各中央企业保密办公室作为本企业保密委员会的日常办事机构，负责依法组织开展商业秘密保护教育培训、保密检查、保密技术防护和泄密事件查处等工作。
第八条　中央企业保密办公室应当配备专职保密工作人员，负责商业秘密保护管理。
第九条　中央企业科技、法律、知识产权等业务部门按照职责分工，负责职责范围内商业秘密的保护和管理工作。

第三章　商业秘密的确定
第十条　中央企业依法确定本企业商业秘密的保护范围，主要包括：战略规划、管理方法、商业模式、改制上市、并购重组、产权交易、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息；设计、程序、产品配方、制作工艺、制作方法、技

术诀窍等技术信息。

第十一条　因国家秘密范围调整，中央企业商业秘密需要变更为国家秘密的，必须依法定程序将其确定为国家秘密。

第十二条　中央企业商业秘密及其密级、保密期限和知悉范围，由产生该事项的业务部门拟定，主管领导审批，保密办公室备案。

第十三条　中央企业商业秘密的密级，根据泄露会使企业的经济利益遭受损害的程度，确定为核心商业秘密、普通商业秘密两级，密级标注统一为“核心商密”、“普通商密”。

第十四条　中央企业自行设定商业秘密的保密期限。可以预见时限的以年、月、日计，不可以预见时限的应当定为“长期”或者“公布前”。

第十五条　中央企业商业秘密的密级和保密期限一经确定，应当在秘密载体上作出明显标志。标志由权属（单位规范简称或者标识等）、密级、保密期限三部分组成。

第十六条　中央企业根据工作需要严格确定商业秘密知悉范围。知悉范围应当限定到具体岗位和人员，并按照涉密程度实行分类管理。

第十七条　商业秘密需变更密级、保密期限、知悉范围或者在保密期限内解密的，由业务部门拟定，主管领导审批，保密办公室备案。保密期限已满或者已公开的，自行解密。

第十八条　商业秘密的密级、保密期限变更后，应当在原标明位置的附近作出新标志，原标志以明显方式废除。保密期限内解密的，应当以能够明显识别的方式标明“解密”的字样。

第四章　保护措施

第十九条　中央企业与员工签订的劳动合同中应当含有保密条款。

中央企业与涉密人员签订的保密协议中，应当明确保密内容和范围、双方的权利与义务、协议期限、违约责任。

中央企业应当根据涉密程度等与核心涉密人员签订竞业限制协议，协议中应当包含经济补偿条款。

第二十条　中央企业因工作需要向各级国家机关，具有行政管理职能的事业单位、社会团体等提供商业秘密资料，应当以适当方式向其明示保密义务。所提供涉密资料，由业务部门拟定，主管领导审批，保密办公室备案。

第二十一条　中央企业涉及商业秘密的咨询、谈判、技术评审、成果鉴定、合作开发、技术转让、合资入股、外部审计、尽职调查、清产核资等活动，应当与相关方签订保密协议。

第二十二条　中央企业在涉及境内外发行证券、上市及上市公司信息披露过程中，要建立和完善商业秘密保密审查程序，规定相关部门、机构、人员的保密义务。

第二十三条　加强中央企业重点工程、重要谈判、重大项目的商业秘密保护，建立保密工作先期进入机制，关系国家安全和利益的应当向国家有关部门报告。

第二十四条　对涉密岗位较多、涉密等级较高的部门（部位）及区域，应当确定为商业秘密保护要害部门（部位）或者涉密区域，加强防范与管理。

第二十五条　中央企业应当对商业秘密载体的制作、收发、传递、使用、保存、销毁等过程实施控制，确保秘密载体安全。

第二十六条　中央企业应当加强涉及商业秘密的计算机信息系统、通讯及办公自动化等信息设施、设备的保密管理，保障商业秘密信息安全。

第二十七条　中央企业应当将商业秘密保护工作纳入风险管理，制定泄密事件应急处置预案，增强风险防范能力。发现商业秘密载体被盗、遗失、失控等事件，要及时采取补救措施，发生泄密事件要及时查处并报告国务院国资委保密委员会。

第二十八条　中央企业应当对侵犯本单位商业秘密的行为，依法主张权利，要求停止侵权，消除影响，赔偿损失。

第二十九条　中央企业应当保证用于商业秘密保密教育、培训、检查、奖励及保密设施、设备购置等工作的经费。

第五章　奖励与惩处

第三十条　中央企业在商业秘密保护工作中，对成绩显著或作出突出贡献的部门和个人，应当给予表彰和奖励。

第三十一条　中央企业发生商业秘密泄密事件，由本企业保密委员会负责组织有关部门认定责任，相关部门依法依规进行处理。

第三十二条　中央企业员工泄露或者非法使用商业秘密，情节较重或者给企业造成较大损失的，应当依法追究相关法律责任。涉嫌犯罪的，依法移送司法机关处理。

第六章　附则

第三十三条　中央企业应当结合企业实际，依据本规定制定本企业商业秘密保护实施办法或者工作细则。

第三十四条　本规定自发布之日起施行。

1.3.5 国家工商行政管理局关于禁止侵犯商业秘密行为的若干规定（1998 年修订）

（1995 年 11 月 23 日国家工商行政管理局令第 41 号发布，1998 年 12 月 3 日国家工商行政管理局令第 86 号修订）

第一条　为了制止侵犯商业秘密的行为，保护商业秘密权利人的合法权益，维护社会主义市场经济秩序，根据《中华人民共和国反不正当竞争法》（以下简称《反不正当竞争法》）的有关规定，制定本规定。

第二条　本规定所称商业秘密，是指不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息。

本规定所称不为公众所知悉，是指该信息是不能从公开渠道直接获取的。

本规定所称能为权利人带来经济利益、具有实用性，是指该信息具有确定的可应用性，能为权利人带来现实的或者潜在的经济利益或者竞争优势。

本规定所称权利人采取保密措施，包括订立保密协议，建立保密制度及采取其他合理的保密措施。

本规定所称技术信息和经营信息，包括设计、程序、产品配方、制作工艺、制作方法、管理诀窍、客户名单、货源情报、产销策略、招投标中的标底及标书内容等信息。

本规定所称权利人，是指依法对商业秘密享有所有权或者使用权的公民、法人或者其它组织。

第三条　禁止下列侵犯商业秘密行为：

（一）以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密；

（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；

（三）与权利人有业务关系的单位和个人违反合同约定或者违反权利人保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的权利人的商业秘密；

（四）权利人的职工违反合同约定或者违反权利人保守商业秘密的要求，披露、使用或

者允许他人使用其所掌握的权利人的商业秘密。

第三人明知或者应知前款所列违法行为，获取、使用或者披露他人的商业秘密，视为侵犯商业秘密。

第四条　侵犯商业秘密行为由县级以上工商行政管理机关认定处理。

第五条　权利人（申请人）认为其商业秘密受到侵害，向工商行政管理机关申请查处侵权行为时，应当提供商业秘密及侵权行为存在的有关证据。

被检查的单位和个人（被申请人）及利害关系人、证明人，应当如实向工商行政管理机关提供有关证据。

权利人能证明被申请人所使用的信息与自己的商业秘密具有一致性或者相同性，同时能证明被申请人有获取其商业秘密的条件，而被申请人不能提供或者拒不提供其所使用的信息是合法获得或者使用的证据的，工商行政管理机关可以根据有关证据，认定被申请人有侵权行为。

第六条　对被申请人违法披露、使用、允许他人使用商业秘密将给权利人造成不可挽回的损失的，应权利人请求并由权利人出具自愿对强制措施后果承担责任的书面保证，工商行政管理机关可以责令被申请人停止销售使用权利人商业秘密生产的产品。

第七条　违反本规定第三条的，由工商行政管理机关依照《反不正当竞争法》第二十五条的规定，责令停止违法行为，并可以根据情节处以一万元以上二十万元以下的罚款。

工商行政管理机关在依照前款规定予以处罚时，对侵权物品可以作如下处理：

（一）责令并监督侵权人将载有商业秘密的图纸、软件及其他有关资料返还权利人。

（二）监督侵权人销毁使用权利人商业秘密生产的、流入市场将会造成商业秘密公开的产品。但权利人同意收购、销售等其他处理方式的除外。

第八条　对侵权人拒不执行处罚决定，继续实施本规定第三条所列行为的，视为新的违法行为，从重予以处罚。

第九条　权利人因损害赔偿问题向工商行政管理机关提出调解要求的，工商行政管理机关可以进行调解。

权利人也可以直接向人民法院起诉，请求损害赔偿。

第十条　国家机关及其公务人员在履行公务时，不得披露或者允许他人使用权利人的商业秘密。

工商行政管理机关的办案人员在监督检查侵犯商业秘密的不正当竞争行为时，应当对权利人的商业秘密予以保密。

第十一条　本规定由国家工商行政管理局负责解释。

第十二条　本规定自公布之日起施行。

第二部分 商业秘密保护合规指引

2.1 指引说明

1.目的

为加强企业商业秘密保护及侵权风险防范意识，宣传和普及商业秘密相关法律知识，为公司制定商业秘密制度奠定良好的基础，根据商业秘密相关法律规定，特编制本指引。

2.适用人员

本指引适用于企业及其下属公司（统称为“企业”）法务人员及各业务部门工作人员。

3.覆盖法域

本指引以覆盖主要业务所在地的原则，介绍了中国的相关规定和实践。

4.使用方法

需要特别说明的是，本指引基于本手册发布之日时有效的法律法规撰写，如所适用法律法规发生变化，本指引中的相关内容可能需要随之修改。同时，本指引仅为一般性的参考及提示资料，不能作为针对任何具体事项或问题的法律意见。为确保具体事项或问题处置的合法、合规及准确性，请进一步咨询法律合规部门或向具有相关资质的内、外部律师寻求法律意见。

2.2 商业秘密法律制度介绍

2.2.1 商业秘密概述

2.2.1.1 商业秘密的范围

在中国，商业秘密保护的信息范围很广，既包括技术信息，也包括经营信息，还包括其他商业信息。可能构成商业秘密的信息包括：设计、程序、产品配方、制作工艺、制作方法、管理诀窍、客户名单、货源情报、产销策略、招投标的标底及标书内容等。

不过，并非所有秘密信息都可作为商业秘密受到法律保护。只有符合以下三个条件的商业信息，才可能构成商业秘密：

- **不为公众所知悉**：作为商业秘密保护的信息应是不为公众知悉的，即在被诉侵权行为发生时该信息所属领域的相关人员并不普遍知悉也不容易获得。
- **具有商业价值**：商业秘密信息应该具有现实或者潜在的商业价值，能为权利人带来竞争优势。

- **采取了保密措施**：权利人应当采取了与保密信息的商业价值相适应的合理措施来防止信息泄露。

2.2.1.2 哪些行为会侵犯商业秘密

在中国，下列行为构成商业秘密民事侵权[1]，严重情况下可能构成《刑法》第 219 条规定的侵犯商业秘密罪[2]：

- 以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他**不正当手段**获取权利人的商业秘密；
- 披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；
- 违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；
- 教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。

此外，经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密。第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。

2.2.1.3 合法获得、使用他人商业秘密的情形

在中国，若通过以下合法手段获知了他人的商业秘密信息，则不属于侵犯商业秘密的行为：

- **权利人自行披露**；
- **自主开发**：通过自主开发，获得了与商业秘密权利人相同或相近似的技术信息或经营信息；

---

[1] 《反不正当竞争法》第 9 条：经营者不得实施下列侵犯商业秘密的行为：（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密；（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密；（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密；（四）教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求，获取、披露、使用或者允许他人使用权利人的商业秘密。经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的，视为侵犯商业秘密。第三人明知或者应知商业秘密权利人的员工、前员工或者其他单位、个人实施本条第一款所列违法行为，仍获取、披露、使用或者允许他人使用该商业秘密的，视为侵犯商业秘密。本法所称的商业秘密，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。

[2] 《刑法》第 219 条：有下列侵犯商业秘密行为之一，情节严重的，处三年以下有期徒刑，并处或者单处罚金；情节特别严重的，处三年以上十年以下有期徒刑，并处罚金：（一）以盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取权利人的商业秘密的；（二）披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密的；（三）违反保密义务或者违反权利人有关保守商业秘密的要求，披露、使用或者允许他人使用其所掌握的商业秘密的。明知前款所列行为，获取、披露、使用或者允许他人使用该商业秘密的，以侵犯商业秘密论。本条所称权利人，是指商业秘密的所有人和经商业秘密所有人许可的商业秘密使用人。

- **反向工程**[3]：对通过合法渠道取得的产品进行拆解与分析，从而推知他人的商业秘密信息。

2.2.1.4 侵犯商业秘密的法律责任

侵犯他人商业秘密不仅有可能承担民事责任和行政责任，还有可能需要承担刑事责任。

- **民事责任：**当人民法院认定侵权成立时，可依权利人请求判令侵权人停止侵权和赔偿损失。对于恶意侵犯商业秘密的行为，将承担相当于补偿性赔偿 1-5 倍的惩罚性赔偿。[4]
- **行政责任：**侵权人需停止侵权，并承担没收违法所得、处以罚款等行政责任。
- **刑事责任**：侵犯商业秘密的行为构成刑事犯罪的，最高可能被判处十年有期徒刑[5]。

2.2.2 何种情况下选择商业秘密保护

2.2.2.1 专利与商业秘密保护的区别

专利是具有实际权属的权利，而商业秘密由于其秘密性并无实际的权属认证。

专利只享有固定的保护期，必须经申请授权并完全公开技术方案，且申请和维护成本可能会很高。一旦被授权后，专利权人便对该技术形成有效垄断，可以阻止他人实施该技术，即使他人是通过自主研发或反向工程而获得该技术的。

与专利保护不同，商业秘密的优势在于有可能获得无限期的保护，且无需申请或公开技术，也无需投入申请、维护成本。但商业秘密一旦被公开，权利就会随之灭失，失去法律保护。最著名的商业秘密案例为可口可乐的配方，至今仍无人知晓其具体成分，已为可口可乐公司带来数十年的持续利润。

---

[3] 该条不适用于集成电路布图设计，对集成电路布图设计进行反向工程而得到与目标集成电路完全相同的布图并投入商业利用的，属于违反《集成电路布图设计保护条例》的侵权行为。

[4] 根据《反不正当竞争法》第 17 条第 3 款：“经营者违反本法第六条、第九条规定，权利人因被侵权所受到的实际损失、侵权人因侵权所获得的利益难以确定的，由人民法院根据侵权行为的情节判决给予权利人五百万元以下的赔偿。”

[5] 根据《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）第十七条规定，侵犯商业秘密，具有下列情形之一的，应当认定为刑法第二百一十九条规定的“情节严重”：

（一）给商业秘密的权利人造成损失数额在三十万元以上的；

（二）因侵犯商业秘密违法所得数额在三十万元以上的；

（三）二年内因实施刑法第二百一十九条、第二百一十九条之一规定的行为受过刑事处罚或者行政处罚后再次实施，造成损失数额或者违法所得数额在十万元以上的；

（四）其他情节严重的情形。

侵犯商业秘密，直接导致商业秘密的权利人因重大经营困难而破产、倒闭的，或者数额达到本条前款相应规定标准十倍以上的，应当认定为刑法第二百一十九条规定的“情节特别严重”。

为保护商业秘密，商业秘密所有者可能需要通过订立保密协议、采取预防措施等手段[6]来对其进行保护。更重要的是，商业秘密不能阻止他人通过自主研发、反向工程获得技术，并且如他人独立获得商业秘密也可以自行申请专利，甚至以该等专利权阻止商业秘密权利人继续使用商业秘密。

下表为专利和商业秘密的主要区别：

	专利	商业秘密
登记要求	经申请、审查后由政府机关授权。	无需经过申请、登记注册程序即可自然取得。
保护期限	20 年（发明专利）、10 年（实用新型）、15 年（外观设计）	无固定期限
保护对象	只能是满足一定条件的技术方案和设计。	除专利保护的技术方案和设计外，还包括了经营方法、市场分析、价格、费用、采购信息、财务计划、招投标材料、特定客户的交易习惯及需求、数据库等经营信息。
对技术的公开要求	须充分公开技术方案内容	未公开的技术信息
举证责任	专利权人依法推定为权利人。	权利人有责任证明商业秘密成立且享有该等权利。
公开技术对权利的影响	可以在符合法律规定的条件下维持权利。	权利人丧失权利。
排他效力	可以阻止他人实施技术。	无法阻止通过自主研发、反向工程获得技术的人实施。

2.2.2.2 专利和商业秘密保护应如何选择

由于经营信息不属于专利权保护的客体，因此只可能通过商业秘密予以保护。

对于技术信息，可以从专利或商业秘密中选择一种保护方式。因此，除了根据本指南第二部分第 2.2.1.2 节提示的各要件判断技术本身是否符合保护条件外，还需结合以下因素考虑如何选择合适的保护策略：

- 该技术信息是否具有专利法所要求的创造性？
- 该技术信息能够在多长时间内保持市场竞争优势？
- 该技术是否容易被公开或他人可以通过反向工程、自行研发获得？

在以下情形时，应倾向于以专利，而非商业秘密保护：

- 技术信息在商业产品/服务中易为公众所接触；

[6] 参见本指引第四部分 4.1.2 节关于第三方侵权的监控及防御性策略的部分。

- 客户不愿签署保密协议；
- 有可能对外进行许可；
- 相关技术人员流动性高；
- 法律法规或政府机关要求公开技术信息；
- 可以预见或已经存在与外部的合作关系；
- 竞争对手很有可能在未来研发出相同的技术。

而在以下情况下，更适合作为商业秘密保护：

- 信息无法通过专利或者著作权保护的；
- 信息是公司的内部信息；
- 信息在公司内部只有少数员工知晓；
- 接触该信息的人员都愿意签署保密协议或承诺书的；
- 竞争者不太可能研发出同样的技术，也不可能从其他渠道获取同样的技术。

2.2.2.3 计算机软件著作权与专利权、商业秘密保护的选择

就计算机软件而言，专利可以用来保护软件功能的各个方面，例如算法框架、软件界面等，而著作权可以用来保护用于实现该功能的软件代码。如果该软件代码被他人盗用，并将其集成到自己的产品中，则既侵犯专利权又侵犯著作权。

商业秘密可以用于保护软件的核心算法、源代码等内容。

2.3 不同场景下的商业秘密风险

2.3.1 自主研发与反向工程

2.3.1.1 自主研发过程中如何避免侵犯他人商业秘密

通过自主研发获得与他人的商业秘密相同的技术/信息，一般不构成商业秘密侵权。但在某些情形下，例如自主研发的团队中招募了原商业秘密权利人的员工并利用了其知悉的商业秘密，也可能引发侵权纠纷。

要避免侵犯他人商业秘密，首先可通过劳动合同、承诺函等形式进行法律责任的规避。如果员工在参与研发过程中认为可能使用了他人商业秘密的，应当主动告知，以便企业及时评估风险和制定应对措施。另外，也要加强对员工的知识产权侵权教育，确保员工遵守企业规章制度，甚至在某些关键项目中或项目的关键技术研发环节，可以考虑将员工的参与限制在与前雇主开发的技术不直接竞争的项目上。这些建议同样适用于企业的合作方（例如其他同业公司、服务公司、高校、研究院、初创型公司、大型科技公司等）。

在实际生产研发过程中，应当注意留存自主研发的相关证据，以证明不构成侵权或者不

构成故意侵权。这些证据包括技术研讨会议记录、技术方案或图纸改进的各个版本、计算机软件算法或代码更新的各个版本等。除了技术成果本身，技术成果的产生时间也应当予以保存。

2.3.1.2 反向工程带来的侵犯商业秘密的风险

通过反向工程获知商业秘密不构成侵权，但反向工程至少需要满足以下条件：

- 载体需通过合法、公开渠道取得：用以进行反向工程的载体，如产品、软件等，应当是通过展会销售、互联网销售或其他公开渠道合法购买取得，对于非公开渠道销售他人所得的产品，或者以租赁、代为保管等方式获得的产品，不宜开展反向工程。另外，对于销售合同中约定“不得进行反向工程”的产品，在进行反向工程时应当谨慎并及时咨询法律意见。
- 技术信息需完全通过反向工程获得：反向工程的实施者应当通过自己的智力劳动，开展拆卸、测绘、分析等研究工作，并由此发现技术秘密信息。以不正当手段知悉他人商业秘密以后再进行反向工程抗辩的，仍然构成侵权。为了避免此种情形，应避免让曾经在前雇主处参与、接触类似技术的人员参与反向工程。
- 对保密信息本身不负有保密义务：实施反向工程的主体应当事先不知道该商业秘密，且对商业秘密权利人不负有保密义务。如果通过雇佣、委托等方式接触和知悉了商业秘密，并与商业秘密权利人签订了保密协议，则不宜开展反向工程。

此外应注意的是，企业在开展反向工程时应留存相关证据，如购买产品的发票、对方的宣传资料、销售渠道信息等，以证明其系通过公开渠道获取反向工程的对象产品；同时应留存反向工程过程中的技术文档，如拆解时或拆解后的产品照片、对产品进行分析的报告和研讨记录等，以证明其对反向工程对象产品实施了研究性工作。

2.3.2 对外合作中的商业秘密风险

在对外合作过程中，无论是上游还是中下游，无论是否签订专门的委托开发或者合作开发协议，任何与第三方的合作都会涉及到商业秘密问题。因此，在开始任何合作之前，明确相关商业秘密问题和风险都非常重要。下方以石油开采勘探行业为例进行说明。

板块	可能涉及的合作
上游产业	• 生产商之间开发新的开采技术； • 涉及境外与当地同业公司的合作； • 生产商与大学、研究机构或其他政府机构合作开发新的开采技术； • 生产商和创业科技公司合作开发新的开采技术； • 生产商和服务公司合作进行开发提高技术水平的技术攻关； • 生产商和大型科技公司之间合作进行公司运营数字化改造，例如支持数字化和云平台的使用； • 各类实体（含公司、高校）之间形成开发和共享技术的产业联合体；

	• 生产商之间合作进行勘探和开采，包括在其他国家/地区与境外生产商进行勘探和开采； • 与院校、科研机构合作开展技术监控和技术检测工作； • 向其他企业定做特定的生产设备、零件等。
中下游产业	• 企业、高校、科研机构之间开发新型储运技术（如新的管线监控技术、新的储运监控技术等）； • 向其他企业定做特定的生产设备、零件等； • 企业、高校、科研院所合作开发供应链优化新技术（如人工智能新算法、区块链供应链管理等）。

在上述合作过程中，如果不在协议中明确商业秘密归属以及保密相关问题，不仅有可能导致企业商业秘密的流失，甚至有可能给企业带来侵权隐患，影响项目的正常业务开展。因此，在对外合作过程中，需要根据企业在合作中的角色关注其中的商业秘密风险。在合作中，企业可能作为技术接收方，也可能成为技术提供方。

身份	合作方
技术接收方	• 与下列实体合作时: o 其他同业公司 o 大学、研究机构或其他政府机构 o 创业公司 o 大型科技公司 o 产业联盟 • 使用开源软件项目时
技术提供方	• 与下列实体合作时 o 其他同业公司 o 产业联盟 • 使用开源软件项目时

2.3.2.1 对外合作时应关注的商业秘密侵权风险

(1) 作为技术接收方应关注的商业秘密侵权风险

在合作过程中，如果需要接收外部技术，需要重点关注以下问题：

- **技术本身的权利瑕疵**

对于合作者提供的技术，应从以下方面进行尽职调查：

- **权属是否有争议**。如果背景技术为合作方的自有技术，那么应调查发明人与技术提供方的雇佣或委托合同关系。如果技术是合作方通过转让或许可获得，或者正处于争议程序中，则更应当仔细审查。
- **权利是否有瑕疵**。重大交易中，如果对方提供的是作为商业秘密保护的技术信息，则应调查是否符合商业秘密的构成要件，例如合作方自身是否采取了适当的保密措施、是否在其他项目中使用、披露过该技术、是否被专利或专利申请公开披露

等。

- **侵权风险评估**。对于实施合作者提供的技术是否存在侵犯第三方商业秘密的风险进行分析和评估。针对上述侵权风险，首先应重点关注合作方是否已就相关技术遭到第三方的侵权警告（口头或书面）、行政投诉及诉讼等。就商业秘密而言，还可关注合作方是否存在从竞争对手处挖核心技术人员等高风险情形，以及相关技术与竞争对手间的相似程度，是否在开发中使用了竞争对手的技术信息及软件源代码等。

- **知识产权条款/条件**

签订合作协议时，需要重点审查与以下内容相关的知识产权条款或条件：

- **合作中产生的新技术合作成果的归属**[7]。约定合作时，应对合作成果的归属予以明确，确保对共同开发或委托开发的知识产权享有权利，应尽量避免约定合作各方共有。如无法约定企业单方享有权利，则应尽量约定企业有权无偿使用相关知识产权。
- **技术成果的使用**：提示合作方未经企业许可，不得使用、公开新成果或将新成果用于申请专利等；
- **确保许可的范围满足项目需求**：以技术许可方式接受技术时，应确保许可范围、地域、领域、时间能够满足项目需求；
- **避免侵犯第三方知识产权**：合作方需保证其提供的技术不侵犯第三方知识产权或未在未经同意的情况下使用开源代码；
- **背景技术的许可**：需确保合作方许可企业，在合作期间及终止后，有权在合同目的范围内使用合作方的背景技术；
- **职务发明相关内容**：合作方应履行对于其员工发明创造的奖励报酬义务，并确保不会有第三方对其知识产权的权属提出异议；
- **第三方知识产权侵权的指控**：合作方应协助企业应对因实施合作方的技术引起的第三方知识产权侵权指控，并提供企业需要的文件、证据及技术支持。如知识产权侵权成立，合作方应赔偿因其侵权行为而给企业带来的损失；
- **是否允许反向工程**：此类条款直接影响企业是否可对技术进行反向工程。

- **新成果的投产、专利申请、公开**

如果合作中产生了新的技术成果，需要根据合同提示合作方相关人员，在企业未确定是否对相关技术信息进行公开以前，不得利用相关信息进行实际生产、申请专利、发表论文或进行其他可能导致技术被公开的行为。

(2) 作为技术输出方应关注的商业秘密风险

在合作过程中，如果需要向第三方提供企业的知识产权，需要重点关注以下问题：

- **知识产权条款/条件**

签订合作协议时，需要重点考虑以下与知识产权有关的条款或条件：

- 明确合作中产生的新技术合作成果的归属[8]。确保企业对共同开发或委托开发的知识产权享有权利，应尽量避免约定合作各方共有。同时，明确约定合作方应及时

[7] 参见本指引第二部分 2.3.2.2 节关于合作中产生的商业秘密归属部分。

[8] 参见本指引第二部分 2.3.2.2 节关于合作中产生的商业秘密归属部分。

就合作产生的新技术成果通知企业；

- 明确许可范围限于项目需求：以技术许可方式提供技术时，应确保许可范围、地域、领域、时间不超出项目需求的必要范围；同时应确保合作方仅在合同范围内使用企业提供的技术；
- 避免就不侵犯第三方知识产权做出保证：任何方式的审查都无法完全排除知识产权侵权风险，所以在签订协议中应尽量避免此类条款出现；
- 第三方知识产权侵权的指控：合作方受到第三方知识产权侵权指控时，应根据企业的指令应对，避免随意向第三方提供任何材料、信息或作出陈述、达成和解等；
- 是否允许反向工程：一般情况下，应要求合作方不得在未经同意的情况下进行反向工程；
- 保密义务：合作方需对企业在合作过程中披露的保密信息承担保密义务。

此外，应避免条款被认定为非法垄断技术的无效条款。[9]

- **新成果的投产、专利申请、公开**

如果合作中产生了新的技术成果，需要根据合同提示合作方相关人员，应及时就合作产生的新技术成果通知企业，且在企业未确定是否对相关技术信息进行公开以前，不得利用相关技术进行实际生产，或者申请专利、发表论文或进行其他可能导致技术被公开的行为。

- **保密信息的保护**

在合作过程中，除要求合作方自身签订保密协议外，还应当要求合作方可以接触企业保密信息的人员签订保密协议、承诺书等。

此外，针对重要的技术信息，也需要不定期地对公开渠道的技术文献进行检查，避免合作方人员在其专利申请、论文、演讲中披露任何信息。

- **防止合作方超范围使用企业的技术**

在合作协议期间或终止后，都应关注合作方是否有超出约定范围使用企业技术，以及合作方是否就合作开发完成的技术实施了侵权行为，例如在约定范围以外的其他项目、地区、时间内使用企业的技术，或者使用企业技术生产的产品数量超出双方约定的限额。

2.3.2.2 合作中产生的商业秘密归属问题

合作中新产生的商业秘密的归属是可以由合作各方约定的。在双方没有明确约定的情况下，将按照法律规定确定新的权利应当归谁所有。在中国，在委托开发、合作开发中完成的技术秘密，各方均有使用和转让的权利。[10]所以，在对外开展合作过程中，需要重视在合同中明确合作产生的新商业秘密的归属和收益。

[9] 参见本指引第二部分 2.2.1 节关于技术条款的合规部分。

[10]《民法典》第 859 条、860 条及《计算机软件保护条例》第 11 条。

2.3.2.3 共有商业秘密的风险

通常情况下,为了更有效地对商业秘密进行行权、许可或出售而无需取得共有人的同意,应避免与他人共有商业秘密。通常更好的做法是由企业作为商业秘密的所有权人,并将使用或利用相关技术所需的权利再许可给另一方,而不是共同所有。

如果共有商业秘密,则可能会遇到以下情形:即使权利人也无法根据自己意愿随意向第三方转让共有的商业秘密。

2.3.2.4 获得商业秘密许可后实施过程中的风险

权利人获得商业秘密并不意味着其可以随心所欲地自由实施,仍然需要判断该实施行为是否会落入他人知识产权的保护范围内。

要防止外部合作带来的侵犯他人商业秘密的风险,主要需关注并避免两种情况的出现:

合作方提供的技术信息是他人的商业秘密。在对外开展合作时,需要合作方明确说明和保证其技术信息来源的合法性。

内部员工使用他人的商业秘密。这种情况多发生在原本就职于同行业企业(包括竞争对手)的新聘员工当中。在有新员工参与项目时,需要提示其避免使用其原雇主的技术信息,并与该员工签署不侵犯原雇主商业秘密的协议。如果需要进行反向工程,还需要特别留意参与反向工程的员工是否原先受雇于被反向工程产品的权利人。

除此以外,在研发过程中,还需要重视保留自主研发、反向工程的过程记录和证据。[11]

2.3.2.5 对外合作中合作方侵犯公司商业秘密的风险

在对外合作过程中,企业可能会向合作方提供作为商业秘密等知识产权保护的技术信息和相关技术资料。如果合作方擅自使用相关知识产权,将给企业的知识产权带来风险。因此,在对外合作中应做到以下几点来控制**商业秘密风险。(信息提供登记表格,请参见附录一)**

落实合作方的保密义务:除要求合作方签订保密协议、承诺书外,在合作过程中应当积极执行、落实保密措施,例如对商业秘密及其载体的交付、外传进行监控、审计、留痕并记录;在研发结束后要求合作方、受托方登记、返还、删除、销毁其接触或者获取的商业秘密及其载体,并继续承担保密义务等。

监控合作方是否有侵权行为:除通过合同约束、采取保密措施外,还需要密切关注合作方是否存在以下几类常见的侵权情形:

- 擅自就技术成果申请专利;
- 将企业的商业秘密或者合作中产生的技术成果用于其他项目或目的;

[11] 参见本指引第二部分 2.1 节自主研发与反向工程部分。

- 未经同意公开、披露、向第三方披露、或者允许第三方使用企业提供的技术信息和资料。

如果发现合作方有上述行为的，应立即向业务主管部门汇报相关事件，并同时通知法律合规部门配合采取维权行动。除此以外，如果发现合作方已经将企业的知识产权申请专利的，则还需要求合作方将相关专利或专利申请转让给企业，以尽可能减小损失。

2.3.2.6 技术跨境使用的商业秘密风险

商业秘密是地域性的。在某个国家/地区实施商业秘密不构成侵权并不意味着在其他国家/地区实施也当然不侵权。如果技术是在国外开发后被引进到中国，那么需要在开发国和中国都考虑商业秘密侵权的风险。反之亦然。

因此，如果需要在多个国家/地区实施该技术，为了最大限度地降低侵权风险，需要分别针对这些国家/地区分别进行 FTO 检索。

2.4 特定技术领域的商业秘密保护

2.4.1 集成电路领域的商业秘密保护

2.4.1.1 集成电路领域现状及特点

近年来，集成电路行业商业秘密侵权案件频发，如上海市公安局侦破的侵犯芯片技术秘密案等。这些案件表明，商业秘密的泄露和侵权对企业造成了巨大损失。因此，企业应高度重视商业秘密保护工作，加强内部管理、完善保密制度、提高员工保密意识等，以防范商业秘密的泄露和侵权。

集成电路行业具有技术密集型、资金密集型、需求多样化、国际竞争激烈和产业链合作紧密等基本特征。这些特征共同推动了电子技术的快速发展和广泛应用，该行业的商业秘密呈现出独特的特点。

技术复合型

集成电路技术的发展涉及多个学科的交叉融合，包括工艺、器件物理、电路设计和 CAD 技术等多个子方向。这些子方向共同构成了集成电路技术全面和合理的格局，覆盖从底层原理到顶层应用的完整技术领域。该行业的商业秘密往往涉及到多种技术领域的复合型知识，不仅包括具体的技术参数和设计图纸，还可能涉及生产流程和材料配方等。这些商业秘密的复杂性要求企业在保护措施上必须具备高度的细致和专业性。

高技术性

集成电路行业是典型的技术密集型行业，其商业秘密往往涉及复杂的技术问题和解决方案。这些技术秘密的获取和保护需要企业具备强大的技术实力和研发能力。因此，集成电路行业的商业秘密具有高度的技术含量和复杂性。

时效性

由于行业技术更新迭代快，某些商业秘密（如早期研究数据）可能随时间推移而失去价值。这要求企业必须不断创新，并及时调整商业秘密保护策略。

人才依赖性

许多关键商业秘密存在于研发人员的头脑中。高素质人才的流动增加了商业秘密保护的难度，要求企业制定有效的人才管理和保密策略。

2.4.1.2 集成电路领域商业秘密的识别

集成电路企业主要可以从以下两个方面识别商业秘密：

企业内部于产品制造过程或特定技术研发生命周期内所产生各种记录，如设计信息、采购技术信息、生产信息、设备设施信息、软件程序等。

企业内部除技术资产之外所涉及的产出成果，包括但不限于战略规划、组织发展、财务管理、产品营销、供应链管理、客户关系管理等生命周期中所产生的各种记录。

具体包括：

涉密技术信息

技术方案、工艺流程、设备图纸、设备参数、项目测试报告、项目规格、项目优化方案、项目实施方案、各模块功能算法、数据接收与反馈方案、接口设计、参数反应模块、平台架构设计、关键技术解决方案、关键设备设计、软硬件整合模块等信息。

涉密经营信息

与经营活动有关的创意、管理、营销、财务、计划、样本、招投标材料、数据、客户信息等，以及对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息。

集成电路领域可能构成商业秘密的内容清单，详见下表。

业务流程	次业务流程	载体	秘密信息				
立项阶段	商务规划	产品提案书	■产品路线图	■竞品比较	■市场区隔	■竞争优势	■产品特色
		市场需求规格 （MRS Draft）	■产品规格	■市场设定	■硬件架构	■功能需求	
	技术评估	技术方案	■技术方案	■设计图	■技术参数	■扩充性数据	■其他数据
		封装选择表 （POT）	■封装方案	■技术规格	■外观设计	■BGA封装	■DIP封装
		成本估算	■IP 面积	■IP 成本	■IP 投资	■生产成本	■测试成本
	立项纪录	立项会议 PPT	■产品规格	■ROI	■市场设定	■产品描述	■目标客户
		项目时程表	■时程规划	■关键人员	■项目章程	■配置管理	■交期控制
		市场需求规格 （MRS）	■产品规格	■市场设定	■行业规格	■市场策略	■可行性评估
开发阶段	硬件开发文件	（各 IP）开发指南	■Feature List	■Feature Dsc.	■参数描述	■编译设定描述	■Power
		计算机设计工具指南	■EDA 工具列表	■操作流程	■参数设定	■物理验证	
		IP 整合指南	■参数清单	■参数描述	■参数设定	■连接设定	
	设计变更通知	（各 IP）设计变更通知	■变更清单	■变更纪录	■变更说明	■其他变更记录	
		软硬件设计变更确认	■变更清单	■变更纪录	■设备参数	■产品规格与式样	■编码架构
	代码开发	硬件代码 （各 IP）	■RTL	■Synthesis	■Netlist	■Bit File	■
		软件代码 （Driver）	■Source Code	■Machine Code	■运行环境	■运行逻辑	■代码架构
	FPGA 测试	测试计划书 （硬件+Driver）	■测试内容	■测试方案	■参数设定	■测试工具	■预估结果
		测试报告 （硬件+Driver）	■问题清单	■解决状况	■运行反馈	■问题优先级	■允许误差
	开发进度纪录	开发进度周报	■开发进度	■问题回报	■负责人员	■历史数据	■对比数据

2.4.2 生物医药领域的商业秘密保护

2.4.2.1 生物医药领域特点

- **高投入**。一个新药从研发到上市通常需要经历数个阶段，历时 10-15 年，投入可能高达数亿甚至数十亿美元。因此生物医药行业有研发周期长、投入大的特征。
- **高风险**。生物医药行业的研发过程不仅投入巨大，还面临着极高的风险。从初始研究到最终上市，每个阶段都存在失败的可能性，使得整体成功率极低。这种高风险特性使得每一个成功的项目都弥足珍贵，相关的商业秘密就成为企业的核心资产。
- **高回报**。成功上市的药物可为企业带来巨大经济效益，专利药在保护期内享有市场独占权，为企业带来高额利润。

2.4.2.2 生物医药领域商业秘密的特点

- **多样性**

生物医药行业的商业秘密涉及研发、生产、临床试验、市场准入和营销等多个环节，包括但不限于：

  - 研发阶段：新药靶点、分子结构、实验数据等；
  - 生产阶段：生产工艺、质量控制方法等；
  - 临床试验：试验方案、临床试验数据等；
  - 市场准入和营销：定价策略、医保谈判价格、准入和市场策略、渠道信息、客户信息等。

- **高技术性**

生物医药行业的商业秘密通常涉及高度专业的科学和技术信息。这些信息往往是长期研究和大量投入的结果，具有很强的技术壁垒，不易被竞争对手模仿或复制。

- **时效性**

由于行业技术更新迭代快，某些商业秘密（如早期研究数据）可能随时间推移而失去价值。这要求企业必须不断创新，并及时调整商业秘密保护策略。

- **价值波动性**

商业秘密的价值可能因研发进展、市场竞争、科技创新、监管环境等因素而剧烈波动。例如，一项临床试验的积极结果可能瞬间提升相关商业秘密的价值，而负面结果则可能导致价值大幅下降。

- **人才依赖性**

许多关键商业秘密存在于研发人员的头脑中。高素质人才的流动增加了商业秘密保护的难度，要求企业制定有效的人才管理和保密策略。

2.4.2.3 生物医药领域商业秘密的识别

鉴于生物医药行业特性，商业秘密往往具有高度的技术性、复杂性和时效性，涉及巨额投资和长期研发成果，贯穿于产品从概念到上市的整个生命周期。准确识别和保护这些商业秘密，对于生物医药企业的长期发展和市场竞争力至关重要。

商业秘密保护部门应评估并识别商业秘密信息，并建立商业秘密清单，确定商业秘密信息、级别、保存期限、涉密人员范围等内容。总体来说商业秘密信息包括：

- 涉密技术信息：与科学技术有关的结构、原料、组分、配方、材料、样式、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；
- 涉密经营信息：与经营活动有关的创意、管理、营销、财务、计划、样本、招投标材料、数据、客户信息等，以及对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息。

一个新药从研发到上市通常需要经历研发阶段、生产阶段、临床试验阶段、市场准入和营销阶段，尽管每个阶段都有其独特的特点和商业秘密保护需求，但在识别和保护商业秘密时，秘密性评估、价值性评估以及保密性评估对所有阶段都是必要的。

(1) 研发阶段的商业秘密

生物医药行业研发阶段的商业秘密可重点考虑以下信息，如新发现的疾病靶点及其验证数据、创新药物分子的化学结构和作用机制、独特的高通量筛选平台和方法、研发过程中产生的实验数据和分析报告、未公开的研发路线图和项目规划、创新的药物递送系统或制剂技术、自主开发的计算机辅助药物设计模型、大分子药物的结构预测和模拟技术等。

- 研发阶段的特点

生物医药行业的研发过程通常包括早期研究阶段、临床前阶段、临床阶段和商业化市场阶段。

- 早期研究阶段：药物研发的最初阶段，主要是基础研究和初步验证。特点是高度创新性和不确定性。这个阶段主要涉及新靶点发现、先导化合物筛选和优化等工作。
- 临床前阶段：药物进入临床试验前的研究，包括药物筛选、动物实验和毒理学研究，以便申请进入临床试验（Investigational New Drug， IND）。重点是药物安全性和有效性的初步评估。这个阶段产生的关键数据，如药效学、药代动力学和毒理学数据，都是重要的商业秘密。
- 临床阶段：包括 1-3 期临床试验，用于在人群中验证药物的安全性和有效性，完成后可以申请上市许可（New Drug Application， NDA）。涉及人体试验，数据的敏感性和价值显著提高。临床试验设计、中期分析结果等都是核心商业秘密。
- 商业化市场阶段：虽然产品已上市，但仍需进行上市后监测、4 期临床试验、适应症扩展研究等。这一阶段的商业秘密保护至关重要，因为企业可能会持续积累关于产品安全性、有效性、市场反馈及潜在新适应症的数据。

- 研发阶段秘密性评估

评估研发相关信息是否已公开。考虑该信息是否已在学术期刊、专利文献或行业会议中披露。特别关注尚未公开的创新性研究成果、实验数据和技术方法等。由于生物医药研发的长周期性，还需考虑信息在整个研发过程中的持续保密状态。

- 研发阶段价值性评估

判断信息是否对企业具有实际或潜在的商业价值，包括但不限于可用于筛选、考虑、确定研发方向，有助于研发策略的制定，提高研发效率等，或与开展或可能开展的研发、

产品开发、权利许可、转让、产品商业化等活动具有关联。考虑到生物医药研发的高风险性和高投入特点，重点关注能够加速研发进程、提高成功率或开拓新市场的关键信息。

- 研发阶段保密性评估

确认企业是否采取了合理的保密措施。考虑是否实施了严格的信息访问控制、与研发人员和合作方签订保密协议、对敏感数据进行加密存储等。特别注意在跨部门协作和外部合作过程中的信息保护措施，以及实验室的物理隔离和安全管理。

(2) 生产阶段的商业秘密

生物医药行业生产阶段的商业秘密可重点考虑以下信息，如优化的发酵工艺参数、大分子药物的纯化和分离技术、创新的制剂配方、独特的质量控制方法、定制化的生产设备设计等。

- 生产阶段秘密性评估

评估生产相关信息是否已公开或易于获取。考虑该信息是否已在专利文件、学术论文或行业标准中披露。特别关注尚未公开的生产工艺、参数优化和质量控制方法等。由于生物医药生产的复杂性，还需考虑信息是否可通过合法的逆向工程获得。

- 生产阶段价值性评估

判断信息是否为企业带来实际或潜在的经济价值。评估该信息能否显著提高产品质量、提升生产效率或降低成本。考虑到生物医药生产的高标准和严格监管，重点关注能够确保产品一致性、满足药品生产质量管理规范（Good Manufacturing Practice，GMP）要求或提高生产灵活性的关键信息。

- 生产阶段保密性评估

确认企业是否采取了合理的保密措施。考虑是否实施了严格的信息访问控制和分级管理，与员工、供应商签订保密协议，对生产区域进行物理隔离和访客管理。特别注意在技术转移、委托生产和质量审计过程中的信息保护措施，以及对关键生产设备和工艺参数的保密管理。

(3) 临床试验阶段的商业秘密

生物医药行业临床试验阶段的商业秘密可重点考虑以下信息，如创新的临床试验设计方案、未公开的中期分析数据和关键的安全性信息、独特的患者招募和筛选策略、自主开发的疗效评估工具、药物序列相关的免疫反应数据、与监管机构的关键沟通记录和策略、创新的统计分析方法等。

- 临床试验阶段秘密性评估

评估临床试验相关信息是否已公开。考虑该信息是否已在临床试验注册平台、学术会议或期刊中披露。特别关注尚未公开的试验设计细节、中期数据分析结果、患者招募策略等。由于临床试验的长周期性，还需考虑信息在整个试验过程中的持续保密状态。

- 临床试验阶段价值性评估

判断信息是否为企业带来经济价值。评估该信息能否影响产品的市场前景、加速审批进程或提高试验成功率。考虑到临床试验的高风险性，重点关注能够降低失败风险、提高成功概率的关键信息。

- 临床试验阶段保密性评估

确认企业是否采取了合理的保密措施。考虑是否实施了严格的数据访问控制、与研究人员和合作方签订保密协议、对敏感信息进行加密存储等。特别注意多中心临床试验中的信息保护措施，以及与医疗机构、合同研发组织（Contract Research Organization，CRO）、现场管理组织（Site Management Organization，SMO）、中心实验室等多方协作过程中的保密管理。

(4) 市场准入和营销阶段的商业秘密

生物医药行业市场准入和营销阶段的商业秘密可重点考虑以下信息，如针对特定治疗领域或地域市场的市场进入策略、详细的客户分析报告、未公开的产品定价模型、精准的市场预测模型、创新的数字营销策略、详细的竞品分析报告、独特的销售渠道管理方法、与战略合作伙伴的会议信息等。

- 市场准入和营销阶段秘密性评估

评估市场准入和营销相关信息是否已公开。考虑该信息是否已在公开报告、行业分析或媒体报道中披露。特别关注尚未公开的市场策略、客户数据、定价模型等。由于市场环境的快速变化，还需考虑信息的时效性和持续保密的必要性。

- 市场准入和营销阶段价值性评估

判断信息是否为企业带来经济价值。评估该信息能否提高产品的市场份额、增加销售收入或提升品牌价值。考虑到生物医药市场的竞争激烈性，重点关注能够提供竞争优势的关键信息。

- 市场准入和营销阶段保密性评估

确认企业是否采取了合理的保密措施。考虑是否实施了严格的数据访问控制、与研究人员和合作方签订保密协议、对敏感信息进行加密存储等。特别注意在与分销商、医疗机构等多方合作过程中的信息保护措施。

2.4.3 网络游戏领域的商业秘密保护

2.4.3.1 网络游戏领域现状

网络游戏以游戏画面为载体，包含了游戏素材、游戏玩法、游戏程序，其中游戏画面和游戏素材是网络游戏的外在表现形式，而游戏程序和游戏玩法是网络游戏的内在表现形式，用户可以在自己选定的时间和地点、播放开发者事先选择或编排好的某部分画面序列。网络游戏行业作为数字经济的核心引擎，其以“互动性”为核心优势，颠覆了传统娱乐的单向输出模式，通过玩家决策塑造动态叙事，协同构建虚实共生的沉浸式娱乐体验。与此同时，知识产权保护跃升成为行业聚焦的关键命题，外挂、换皮、泄密等技术性侵权与全球化规则博弈交织，倒逼行业从“规模红利”向“质量红利”转型。未来，随着 AIGC 技术深度应用与政策法规完善，网络游戏行业将在技术赋能与文化输出的双轨中，持续释放新质生产力的战略价值。

2.4.3.2 网络游戏领域商业秘密的特点

网络游戏保护领域，经营信息的形态发生显著变化，主要呈现为以数据集合的形态存在的游戏代码、数值设定等，以及以可视化形式承载的游戏角色形象、技能效果、地图地标、剧情画面等。

一方面，在民事案件中，法院多依据秘密性、价值性、保密性三要件将网络游戏未公开信息依法定性为商业秘密。例如，上海市浦东新区人民法院(2024)沪 0115 行保 2 号与(2024)沪 0115 民初 38294 号案件中，涉及游戏未公开角色的实际形象和技能效果等信息是否属于商业秘密的判断，上海市浦东新区人民法院认为：“该未公开信息系权利人在经营活动中通

过长期不懈努力的创新创造和积累所获得的信息”及“对权利人开展经营具有核心竞争价值”，与“游戏经营者不断更新迭代并对未公开内容保密以维持热度的长线经营策略”及“商业模式使得该信息具有纳入商业秘密保护的必要性”，判断这类信息符合经营信息的基本特征，具有纳入商业秘密予以保护的现实必要性，认定网络游戏未公开信息为反不正当竞争法所保护的商业秘密。又如，上海市徐汇区人民法院（2024）沪 0104 民初 12537 号案件中，上海市徐汇区人民法院认为未公开游戏信息能够用于经营、给权利人带来竞争优势，属于“经营信息”。

另一方面，由于经营信息存在规范性要素特征，要考虑事实、研发、政策等多种因素，尚缺乏认定游戏经营信息商业秘密的刑事案例。从实践情况看，对获取、披露、使用或者允许他人使用网络游戏未公开信息的行为，刑事司法部门在立案追诉环节可能持保守谨慎的观点。首先，将此类信息定性为商业秘密存有一定难度，这种未公开的游戏信息是阶段性保密信息，很快就会公之于众。游戏行业研发具有明显的迭代性特征，单个版本的平均生命周期仅为 6-8 个月，定期迭代的“未公开信息”具有重要的商业价值，这在以追求内容创新为特色的游戏公司尤为明显，“阶段性”的保密会影响经营信息的定性吗？其次，对著作权保护与反不正当竞争保护之间的关系，实践中有观点倾向于著作权法优先，因此可能会建议权利人基于美术作品维权等分拆保护思路，如此一来，未公开信息中的核心玩法规则、经济系统参数等非可视化要素难以获得充分保护。

2.4.3.3 网络游戏领域的商业秘密侵权纠纷类型

根据网络游戏的营运周期特征，可将网络游戏涉及的知识产权纠纷的主要类型分为三个阶段：游戏研发阶段、游戏运营阶段和宣传推广阶段。

其中，游戏研发阶段是商业秘密侵权发生的主要阶段。在游戏研发阶段，游戏代码、核心玩法、美术素材等信息关乎游戏的市场竞争力。此阶段的商业秘密侵权案件主要集中于游戏代码侵权和游戏内容泄密。

(1) 游戏代码侵权

代码编写是游戏制作的重要环节，游戏代码是实现游戏运行的工具。源代码作为游戏正常运行的“安身立命之本”，一旦泄露，将对游戏造成毁灭性打击，将其作为商业秘密加以保护属于题中应有之义。

泄露游戏源代码构成侵犯商业秘密的认定：判断被诉侵权人的行为是否侵犯商业秘密，不能仅孤立地看被诉侵权人此前有无接触、获取商业秘密的权限和被诉侵权人获取商业秘密的方式是否对应法律明文列举的手段类型，而应当综合审查被诉侵权人获取商业秘密的意图及其获取商业秘密后实施的行为，判断该被诉侵权行为是否导致或者可能导致权利人失去对该商业秘密的有效控制。

(2) 游戏内容泄密

游戏上线或更新前存在游戏未公开信息泄露的风险。尚未公开的游戏内容是否属于经营信息成为影响权利保护的难题。实践中，此类未公开的诸如角色素材、活动剧情等游戏内容可被认定为商业秘密，从而加以保护。在判赔数额上，法院的支持保护力度也逐渐加大。

- 未公开地图、地标、剧情等可构成商业秘密：关于网络游戏内容是否构成商业秘密。首先，涉案信息是否属于反不正当竞争法中规定的经营信息。其次，涉案信息是否不为公众所知悉、是否采取相应保密措施。再次，涉案信息是否具有商业价值。

- 未公开角色、新版本活动等可构成商业秘密：尚未公开的游戏更新内容是游戏产业能不断吸引客户、保障商业模式持续运转的核心组成部分，能够为原告带来现实和潜在的商业价值，且未对外公开，并不为公众所知悉且权利人采取签署保密协议等保密措施的，可以将其认定为“经营信息”。
- 未公开角色、技能效果等构成商业秘密的认定：游戏未公开角色设计符合商业秘密“三要件”，即秘密性、价值性、保密性，属于反不正当竞争法所规定的经营信息，具有纳入商业秘密予以保护的现实必要性。
- 以电子入侵方式窃取游戏未公开内容：通过电子入侵方式窃取他人尚未公开的游戏内容来谋取私人利益，侵犯了他人的商业秘密，构成不正当竞争。

2.4.4 人工智能领域的商业秘密保护

2.4.4.1 人工智能领域现状

人工智能是一个多学科交叉融合的新兴科学领域，近年来发展迅猛。人工智能正引领新一轮的科技革命和产业变革，成为发展新质生产力的重要引擎。国家不断鼓励核心硬件产品自主研发，鼓励大型企业加大 5G、大数据人工智能等数字化技术应用力度，支持工业人工智能芯片、工业视觉传感器等基础硬件的研发突破。围绕人工智能形成了基础层、框架层、模型层、应用层的产业链结构。

- 人工智能行业

  人工智能是人类发展的新领域，人工智能行业是指以人工智能技术研发为重要业务，直接从事人工智能产品或服务创造的企业组成的产业链。包括研究和开发计算机视觉、智能语音、自然语言处理、生物特征识别以及虚拟现实等人工智能技术层的科技企业和科研院校，也包括专注于行业场景应用软件开发的企业。

- 人工智能产业链

  人工智能产业链包括基础层、框架层、模型层和应用层四个部分。基础层主要包括算力、算法和数据、芯片和硬件基础设施建设；框架层主要是指用于模型开发的深度学习框架和工具；模型层主要是指大模型等技术和产品；应用层主要是指人工智能技术在行业场景的应用。

2.4.4.2 人工智能领域商业秘密的特点

人工智能技术涉及的领域广，技术迭代快，国际交流合作频繁。开源人工智能技术、人工智能供应链具有全球化的特点。人工智能行业发展，不可避免地会在全球范围内共享人工智能知识成果。算法透明和开源技术与商业秘密的保护之间存在矛盾。人工智能行业的商业秘密保护需要寻求保护创新和商业利益二者之间的平衡。

人工智能行业人才稀缺，人员流动也是促进行业发展的重要因素之一。企业既要重视商业秘密保护，又要兼顾人才就业权的保障。

人工智能行业的技术秘密更多以电子化和数据化形式存在，容易通过非法下载和信息网络传输实现信息转移。

2.4.4.3 人工智能行业商业秘密的重要性

- 人工智能的行业意义

人工智能行业对我国加快建设成为制造强国、网络强国和数字中国至关重要。人工智能与其他行业融合的特定场景创新，又能引领其他产业的迅速升级和变革。只有对人工智能技术创新成果加以保护，让人工智能知识产权价值得以体现，才能吸引更多的人工智能技术人才专注于人工智能前沿基础理论的创新和关键核心技术的创新，吸引更多企业加大投入，促进行业快速发展。

- 商密保护的法律意义

在法律保护途径上，人工智能可能通过著作权、专利权和商业秘密等三种方式保护，其中商业秘密对于人工智能保护具有巨大意义。

人工智能著作权保护的客体只能以代码化指令序列文字等方式呈现，而不包括任何无法直观展现的算法思想、操作方法等。人工智能专利保护的客体也不能是单纯的算法，而必须是能够与技术特征相结合的技术解决方案。

商业秘密不需要形式上的完整性，任何模块或解决方案的实用信息都可以商业秘密的形式获得保护。所以商业秘密保护对于人工智能行业创新成果的著作权保护和专利权保护构成了非常有益的补充。

2.4.4.4 人工智能领域商业秘密的识别

企业应根据自身的技术类型和所处人工智能产业链中的位置，对经营中形成的技术信息和商业信息进行识别，建立商业秘密清单，确定商业秘密信息、级别、保存期限、涉密人员范围等内容。包括：

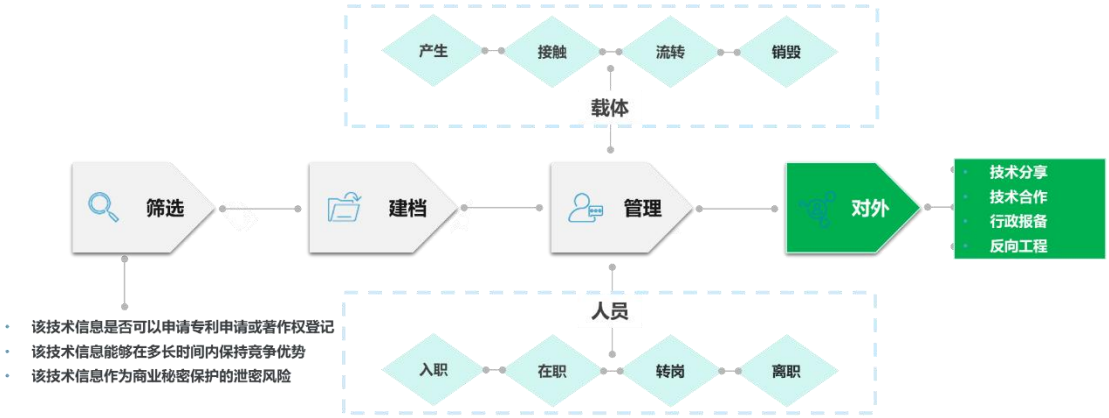
- 技术信息
  - 基础设施及硬件：具有创新性的芯片架构等；
  - 软件信息：关键人工智能程序代码、源代码、应用程序、系统软件等；
  - 算法和模型：独特的算法设计、数据训练方法、基础框架设计、基础大模型设计、调优方案、模型架构和参数等；
  - 数据：经过训练的数据、独特的数据技术、经过标注或具有独特价值的数据集、测试数据和验证数据等；
  - 研发信息：记录研发过程、技术思路、实验结果等的研发文档、技术报告和系统设计图纸，尚未公开的研究方向、创新想法等；
  - 技术方案：针对人工智能应用的技术解决方案，提升系统性能的独特策略和技巧等。
- 经营信息：与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息等。
  - 客户信息：对特定客户的名称、地址、联系方式、交易习惯、交易内容、特定需求等信息进行整理、加工后形成的客户信息。
  - 经营决策：战略决策、研发策略、研发方向与领域、投资、股权激励方案、技术规划布局、营销策划、营销方案、预决算报告、信息安全风险报告、运维日志等。
  - 行业分析：人工智能市场的深入分析和市场预测数据、需求趋势预测、重要客户的特殊需求分析等。
  - 场景需求：特殊的场景需求、尚未公开的场景创新。

人工智能领域可能构成商业秘密的评估方式，详见下表。

	秘密性评估	价值性评估
基础层企业	核心算法、数据处理技术、硬件设计和制造工艺等是否不为公众所知悉。尤其是经过大量的研发和实践积累的特定的高效数据清洗算法、数据存储架构设计、特定的芯片架构、高性能服务器的内部构造等。	该技术是否能提高数据的处理和存储效率，是否可以提升人工智能模型的训练和推理速度，以及为上层提供稳定的计算能力等。评估基础层的技术创新的成本与投入，及一旦被公开可能导致企业的商业价值或竞争优势减损。
框架层企业	开发框架的独特架构和优化策略是否不为公众所知悉，尤其是框架实现高效的并行计算、内存管理等技术细节，框架的接口设计和扩展能力等。	框架是否能创造高效的开发环境，降低人工智能模型开发的难度和节约成本。评估框架的商业和竞争力价值。
模型层企业	模型的结构和参数组合是否为公众所知悉，模型的训练数据和训练方法是否为公众所知悉。	模型是否能为企业带来商业价值，尤其是在图像识别、自然语言处理等方面是否能提高生产效率、改善用户体验。评估模型的不断改进和优化是否可以保持企业在市场中优势地位。
应用层企业	在特定行业的应用解决方案和业务流程是否为公众所知悉，场景应用的创新是否尚未公开，用户数据分析和处理方法是否具有独特性、秘密性。	应用场景是否提高了行业效率，提高了性能，降低了开发成本等，应用层的创新对于开拓新的市场和业务领域的商业和竞争价值。

2.5 商业秘密的日常管理

2.5.1 管理思路



(1) 筛选

- 确定商业秘密保护认定机制，即对企业运营过程中所产生的海量信息进行筛选，甄别出有保护价值的信息；
- 确定知识产权保护策略选择机制，从有保护价值的信息中分别甄选出作为专利保护及/或商业秘密保护及/或著作权保护的信息。

(2) 建档

- 对商业秘密信息进行建档管理，对技术信息的技术优势、实质性特点形成模板文件，目的是从商业秘密实例中归纳出商业秘密信息的保护范围；
- 对商业秘密进行密级的适当划分与确定，包括在建档、保存过程中对商业秘密载体的保全和存证。

(3) 载体管理

- 建立对商业秘密载体及涉密人员的管理制度，包括针对数据及载体的产生、接触、流转、销毁等环节的登记和留痕，对人员权限的合理设定及访问控制等，设置文件管理制度、IT 管理制度等。

(4) 人员管理

员工作为接触商业秘密的人员，应当受到严格的管理，具体而言，应当关注员工从进入企业至离开企业的所有阶段：

员工入职管理：

- 在新员工入职时进行背景调查，尤其关注有保密义务、竞业限制义务的员工；
- 建立和完善商业秘密相关的制度、合同等（包括但不限于员工手册、劳动合同、保密协议、保密制度、竞业限制协议、期权协议等），同时进行相关的培训。

员工在职及转岗管理：

- 建立日常商业秘密保护相关的合规流程，监控员工的异常事宜；
- 如发生泄露商业秘密等相关事宜，进行调查，搜集相关证据并采取相关措施。

员工离职管理：

- 建立离职流程，监控员工离职时是否有异常情形，及时审查离职员工是否履行竞业限制义务，以便有效实现商业秘密保护目的；
- 如发现商业秘密侵权或违反竞业限制的事宜，及时搜集相关证据，有效采取法律措施。

(5) 对外合作

- 建立对外合作中的保密制度，包括对外合作前的保密协议起草及签署、对外提供技术资料或技术分享内容的审核、对外提供文件的涉密标识、对外销售产品的保密措施（如签署保密协议、在相关场所设置保密标识、在产品中设置防止反向工程的物理保密措施等）。

(6) 监控与管理

- 定期审计上述商业秘密筛选、建档及管理情况，并加以改进。

(7) 重大交易过程中的商业秘密尽调

- 在涉及重大知识产权交易中安排商业秘密尽职调查。

2.5.2 人员管理

2.5.2.1 员工入职管理

企业员工入职时的商业秘密管理可以在企业面临潜在的侵权指控时有效降低侵权风险，同时，通过商业秘密管理实现对企业自身商业秘密的保护：

- 企业可以对入职员工是否存在刺探本企业商业秘密目的进行仔细甄别，防范商业秘密泄露风险；
- 企业应当与员工签订保密协议，明确员工对公司信息负有保密义务。

2.5.2.2 员工在职管理

企业应建立在职员工商业秘密培训体系，包括但不限于：

- 对核心员工进行商业秘密警示性培训，以刑事犯罪和高额侵权赔偿案例提高核心员工对商业秘密管理制度的依从性；
- 对企业高管进行商业秘密泄密事件影响企业正常经营和发展的案例分享和培训，提高企业对商业秘密保护的重视度；
- 对法务进行商业秘密专业培训，详细分析商业秘密保护具体法律问题的理解和适用；
- 对所有员工进行商业秘密法律知识普及和企业商业秘密管理制度培训，树立商业秘密保护意识；
- 企业商业秘密培训应当要求员工签到、签收培训资料，并妥善保管。

企业应建立在职员工商业秘密访问权限管理体系，包括但不限于：

- 企业应当根据员工接触的项目和产品、职位的角色和等级确定其访问和接触相关商业秘密的权限，权限授予应当遵循“最小必要”原则；
- 企业应当根据密级的不同设定不同的授权方式，例如高密级商业秘密可以单独审批、按次审批；一般密级的商业秘密可以分阶段授权，定期检查；低密级商业秘密可以对确有必要访问的员工长期授权；
- 在可能的情况下，企业可以限定员工只接触商业秘密的一部分，避免各岗位相关人员接触到岗位范围之外的其他涉密信息，避免一个员工完整地知悉某一完整经营环节的所有涉密信息；
- 企业应建立商业秘密授权动态调整机制，项目终止或员工转岗之后，应当及时调整权限，如定期（季度/半年）核查员工权限，并进行调整；
- 员工离职时应当及时关闭权限；
- 员工的权限授予、变更和取消应当进行妥善记录和保管。

企业应当通过员工手册及公司制度约束可能的商业秘密侵权行为：

- 企业应当在员工手册、公司制度中明确告知员工对企业信息负有保密义务；
- 企业应当在员工手册、公司制度中明确告知员工公司禁止的数据传输方式及其他禁止的数据复制、下载、传输、访问行为；
- 企业应当确保员工签收公司员工手册和公司制度，在员工手册和制度有更新的情况下，应当要求员工签署更新版，对签署、交付、告知的记录应当予以留档。

2.5.2.3 员工离职管理

企业应当建立员工离职调查机制，包括：

- 对离职员工的潜在侵权行为进行调查：
  - 检查员工是否存在异常操作，例如高频次访问涉密文件，大量下载、拷贝、打印涉密工作文件等；
  - 应当重点监控员工离职前一定期限内对涉密文件、数据的接触情况；
  - 对于明确有侵权行为的，应当留档记录，条件允许的可以及时进行公证或其他证据保全措施；
- 对可能存在侵权行为的员工进行访谈并签署相关文件：
  - 通过访谈与员工确认是否确实存在该等潜在侵权行为，该等行为的目的等，并要求员工签署访谈记录；
  - 要求员工对过往的潜在侵权行为和相应记录进行确认和签署；
- 对于离职员工，企业应当要求员工登记、返还、清除、销毁其获取的商业秘密及其载体，可以对电脑交接进行公证；
- 企业应当告知保密义务并要求员工承诺不会披露、使用、允许他人使用商业秘密，视情况要求重要岗位员工或掌握核心机密的员工签署《保密协议》、《竞业限制协议》等文件。

2.5.2.4 访客管理

企业应当设置访客管理制度，相应管理措施可以包括：

- 要求访客进行实名登记，记录访问时间、目的、邀请人；
- 制作并发放访客登记卡，或者其他能够明确识别其访客身份的标记；
- 访客需受邀并有专人陪同方可进入公司区域；
- 访客进入保密区域需申请审批，并提醒访客注意相关保密义务；
- 对访客的身份、每一次进出及时长均予以记录并保存。

2.5.2.5 合作方管理

企业应建立合作方商业秘密管理机制，此处的合作方可能包括：

- 技术开发和转让过程中的受托开发方、合作开发方、委托开发方、技术受让方、技术转让方等；
- 企业正常经营过程中的供应商、经销商、代理机构、委托加工方、定制加工方等；
- 企业委托的第三方机构，例如技术鉴定方、技术评审方、咨询公司、律师事务所、会计师事务所、资产评估机构等；
- 企业融资、兼并收购中的投资人、中介机构等；

合作方商业秘密管理过程中，企业应当注意：

- 应当在披露任何信息前，与合作方签订保密协议，明确保密义务和违反保密义务的违约责任；
- 根据商业秘密的密级确定访问限制措施，例如：
  - 高密级文件仅允许现场查看，不得复制、摘录、传输，或仅允许在线访问数据库中文件，不得下载、编辑、复制；
  - 其他密级文件可以采取对电子载体加密等方式访问；
- 传输的内容和具体接收文件的主体应当符合“最小必要”原则，不必要的信息可以进行遮盖处理；
- 对于样机、样品等，应当要求合作方不得披露，并要求限期返还或销毁。

2.5.3 保密信息管理

2.5.3.1 商业秘密识别

企业应当建立健全商业秘密识别机制。商业秘密识别机制是指企业在经营过程中找出并确定属于商业秘密的信息。

- 建立动态识别机制：对技术信息而言，在研发项目立项、中期、验收、受托开发方交付、阶段性反馈等环节，应当对过程中涉及的技术信息进行识别，判断是否构成商业秘密；对经营信息而言，在经营信息定稿、签批、提交等环节，判断是否构成商业秘密；
- 建立定期识别机制：企业可以以月度、季度、半年为固定期间，对在此期间产生的技术信息和经营信息进行汇总和整理，判断是否产生新的商业秘密；
- 企业应当根据业务需求，采用适当的商业秘密识别机制：
  - 对于重要项目可以将动态识别机制作为主要方式，以定期识别机制作为补充；
  - 对于一般项目可以采取定期识别机制；
  - 对于重要性较低的项目可以在项目完结后识别，或以较长的识别周期定期识别。

2.5.3.2 商业秘密分级

企业对商业秘密实行分级保护制度。商业秘密的分级可以包括秘密、机密、绝密等等级，企业可以根据实际经营情况调整分级方式；

商业秘密分级时可以考量的因素包括：

- 企业为获得商业秘密所投入的资源和成本；
- 商业秘密泄露后可能给企业造成的经济损失和竞争利益的损失；
- 商业秘密泄露后可能给竞争对手带来的获利或竞争利益；
- 他人独立开发、反向工程等商业秘密的难易程度；

企业应当根据商业秘密的密级确定相应的保护措施。商业秘密分级制度的目的，在于使企业将有限的资源优先投入高密级商业秘密的保护中，并适当降低低密级信息的保护成本，整体上提高商业秘密保护的效率。

2.5.3.3 商业秘密载体录入和保密标记

企业应当将经营过程中产生的可能构成商业秘密的信息录入载体。员工记在脑海中的知识和口口相传的涉密信息，一般难以作为商业秘密主张。因此，在企业完成商业秘密识别之后，应当及时采用合适的载体记录商业秘密。

商业秘密载体包括纸介质、磁介质（包括计算机硬盘、软盘、U 盘、移动硬盘、磁带、录像带等）和光盘等各类可记载文字、数据、符号、图形、图像、声音等信息的物质。一般可以区分为电子载体（例如保存在服务器、计算机、存储设备中的电子文档）和物理载体（例如纸质图纸、书面文件、机器设备、样机等）。

商业秘密在录入载体后应当添附明确的保密要求、保密标记，并采取合理的保密措施。

对被识别为包含商业秘密的载体，应建立商业秘密台账进行记录。商业秘密台账中应当记载的信息包括：载体名称、创建时间、密级、可能的涉密信息等。商业秘密台账中可以声明，台账记载的商业秘密载体并非对所有商业秘密载体的穷尽式列举，其他与记载载体相同或实质性相同的商业秘密载体，以及企业未及时录入的载体，符合商业秘密构成要件的，仍作为企业的商业秘密保护。

2.5.3.4 商业秘密的保密期限及保密措施

保密期限

企业自行设定商业秘密的保密期限。可以预见时限的以年、月、日计，不可以预见时限的应当定为“长期”或者“公布前”；

保密期限的设定，是企业基于保密成本考虑，对保密措施的持续期间作出的预估。对于维持保密措施的成本较低的载体文件，可以不设定保密期限；

对于设定保密期限的商业秘密，应当声明或规定，保密期限是企业对该等商业秘密保持非公知性时间的合理预估，对于保密期间经过，但仍有非公知性和价值性，且企业持续采取保密措施的，视为保密期限自动延长。

保密措施

对于完成识别、定级、录入的商业秘密及载体，企业应当采取合理的保密措施。一般认为，保密措施可以从以下方面落实：

- 主体管理：员工管理（包括入职管理、在职管理、离职管理）、访客管理、合作方管理等；
- 客体管理：电子载体管理、物理载体管理等；
- 接触媒介管理：涉密区域管理、门禁管理、信息系统管理等。

企业可以根据实际经营情况选用合适的保密措施。

2.5.3.5 商业秘密电子载体管理

企业应建立商业秘密电子载体管理制度，包括：

- 企业应当对电子载体设置保密标识：在涉密电子文档文件名上标注“涉密”等字样，并在涉密电子文档首页、页眉、页脚、页面水印等处设置保密义务提醒；
- 企业应当对商业秘密电子载体采取安全措施：设置单独的服务器用于存放涉密电子文档，对能够接触或获取商业秘密的计算机设备、电子设备、网络设备、存储设备、软件等采取禁止或者限制使用、访问、存储、复制等措施；
- 企业应当对商业秘密电子载体采取访问限制措施：对员工采用数据防泄漏系统，对访问、上传、下载、删除、编辑等一系列行为进行记录并予以保存，并对任何数据泄露事件有实时警告，定期核查系统记录的商业秘密泄露事件；
- 对核心员工采用一定的技术手段，对大规模、频繁的异常数据传输事件进行监控与核查；
- 对涉密电子载体打印进行限制：采取涉密文件打印审批制度，经批准后方可打印，妥善保存打印记录，并对纸质打印件进行管控；
- 对涉密电子载体（电脑、服务器、U 盘、存储介质、机房中的电子数据等）进行加密，采用复杂密码，密码和文件分开传输；
- 设定 USB 使用规范：采用技术手段全面封禁 USB（或者只能拷入，不能拷出），仅对特殊需要的岗位配备公司加密 USB，但严禁使用个人 USB，且对每次使用均予记录并保存；
- 就网盘及特定域名进行封禁：采用实际手段全面封禁第三方网盘和特定域名（网页版聊天工具等），并提供公司安全的网络传输工具，对传输记录留痕；
- 企业应当通过提供加密文件传输工具、内部安全传输系统，以及快速简化的审批流程，最大程度减少保密措施给工作带来的不便。

2.5.3.6 商业秘密物理载体管理

企业应建立商业秘密物理载体管理制度，包括：

- 对涉密信息物理载体设置保密标识，在文件、设备上标明“保密”字样并标明密级；
- 对物理载体采取保密措施，将图纸、设计文档、产品样机等物理载体集中管理，放置于特定区域，并限定并记录物理载体数量，对必要的复制、复印、打印、扫描、借阅、借用等行为进行登记并予以保存；
- 对商业秘密实体载体的打印流程做出规定：根据企业内不同工作人员的工作需要，配备专用或公用的打印机，或设定不同的使用权限，对打印、扫描的文件与份数进行登记并予以保存。

2.5.3.7 保密区域管理

企业应当设置保密区域：

- 企业应针对涉密的厂房、车间、实验室、财务室等生产经营或研发场所采取保密措施，严格限制进入权限；
- 保密区域应与一般办公场所区分管理，在必要情况下设置警卫岗哨；
- 在出入口设置门禁，不同区域设定不同的进入权限，对进出记录进行保存；
- 在主要公共场所设置监控摄像头，并在一定期限内保留监控记录；
- 企业设置专门的保密区域存放涉密文档：将涉密文档置于统一区域集中管理，注明保密标记和保密要求，设定门禁和监控；对确有需要接触涉密文件的，采取审批手续并严格监督。

2.5.3.8 对外披露活动中的商业秘密管理

本指引所称“对外披露活动”包括：产品上市销售、展会展出、专利申请、论文发表等场景。

在对外披露活动中，企业应当进行商业秘密审查，包括：

- 在产品上市销售前，企业应当对产品中载有的技术信息进行评判，选择适当的保护策略进行保护，有以下情形的，不建议通过商业秘密进行保护：
  - 产品上市后能够通过直接观察、简单拆解即可获得相应技术信息的；
  - 产品上市后能够轻易地通过反向工程即可获得相应技术信息的；
  - 通过产品的功能实现，可以轻易地独立开发相应技术方案的；
  - 其他不适宜通过商业秘密进行保护的场景；
- 在专利申请前，应当考量专利保护的公开性、对世效力和期限性，以及商业秘密保护的秘密性、相对性、永久性，选择合适的保护方案；
- 在论文发表、展会展出前应当通过保密审查删除涉密部分，避免潜在的技术方案通过论文发表或展会展出进入公有领域。

2.5.4 商业秘密与人员分级的综合管理

2.5.4.1 商业秘密管理机构

企业应当指派特定的人员和组织负责商业秘密的管理工作。商业秘密管理机构可以包括：

- 商业秘密决策部门：负责审批商业秘密方针、制度、政策，重大泄密事件的应急处理，调配商业秘密管理所需资源等工作；

- 商业秘密管理部门：负责制定商业秘密方针、制度、政策，一般泄密事件的处理，协调管理各部门商业秘密管理的工作职责，处理商业秘密员工管理、争议解决、培训教育等具体工作；
- 各业务部门的商业秘密负责人：负责本部门的商业秘密方针、制度、政策的执行，根据商业秘密管理部门的协调执行工作职责，协助商业秘密管理部门处理员工管理、争议解决、培训教育等具体工作。

各企业可依据自身情况增加或减少管理机构层级，并明确各个层级的职责分工。

2.5.4.2 人员与商业秘密密级的匹配

企业应根据业务模式、研发模式、对外合作模式等确立商业秘密与人员岗位的匹配管理模式。一般有以下两种匹配模式：

- 根据职级、部门、工作所需接触涉密信息的程度，将人员密级与保密信息接触权限进行匹配；
- 根据具体项目涉及保密信息的重要程度，对项目信息接触人员的密级进行管理。

在以上两种情况下，都应对不同部门、不同项目间的商业秘密访问权限进行隔离。

2.5.4.3 侵权风险应急管理

公司在生产经营过程中，存在发生商业秘密泄露的风险，失密、泄密事件会造成公司经济损失，为公司生产经营带来负面影响。为提高发生失（泄）密事件应急处置能力，最大限度地减少失（泄）密事件所造成的损害，公司应制定应急处理预案。

应急处理预案至少应包括以下内容：

- 失（泄）密事件的应急管理小组；
- 失（泄）密事件的具体负责人；
- 发生失（泄）密事件后的汇报内容：通常应包括部门，涉及商业秘密的范围、密级、数量及载体，事件发生（发现）的时间、地点、简要过程等，已造成或可能造成的危害，已采取或拟采取的办法和补救措施；
- 失（泄）密事件的处置预案；
- 失（泄）密事件结束后的通报处理、警示教育。

2.6 商业秘密侵权风险在不同情形下的应对策略

2.6.1 第三方侵犯企业商业秘密的风险及应对策略

2.6.1.1 第三方侵权的高风险情形

企业发生第三方侵权的高风险情形主要集中在以下两种侵犯商业秘密行为：

(1) 员工离职带走商业秘密

部分技术岗位人员流动率高，增加了商业秘密被非法窃取和披露的风险。泄密风险主要发生在跳槽员工能够接触到并实际掌握公司核心秘密的情形，例如高级技术主管、核心研发人员或管理层。他们把在原单位的核心技术信息带到新单位使用或申请专利，或者新设公司利用在原单位掌握的核心技术信息从事经营活动。

(2) 合作方泄露商业秘密

企业在日常经营中可能与不同的合作方，例如其他同业公司、大学、研究院、初创公司、大型科技公司等进行合作。在合作过程中，企业可能会提供、分享相关技术、经验和知识产权，因此存在合作方超出许可范围使用企业知识产权或未经允许非法披露企业商业秘密的风险。

例如，在委托第三方提供检测和维修服务或者在向第三方购买定制化的专用设备时，可能需要向该第三方提供关键技术参数、设计图纸等。另外，企业在向非关联公司提供该技术设备、服务时，服务接收方也有机会接触到企业的商业秘密信息。接触到商业秘密信息的人员增多，也提高了商业秘密被泄露的风险。

2.6.1.2 第三方侵权的监控及防御性策略

针对第三方侵权的监控及防御性策略包括：

- 在商业秘密载体文件上标注权属：在企业的技术文件上标注企业名称或标识以及“保密”字样以明示商业秘密的权利归属。
- 监控竞争对手的知识产权使用行为，主动使用技术工具标记知识产权资产或用于证明后续的侵权行为。
- 利用行业相关资源来调查和监控竞争对手的商业活动。监控手段包括：
  - 定期关注竞争对手的网站或社交媒体平台；
  - 参加展会、行业或学术会议；
  - 对竞争对手产品进行反向工程；
  - 对竞争对手新发布的技术出版物进行监控；
  - 必要时，可以考虑购买相关产品，进行侵权分析。

- 利用知识产权数据库检索竞争对手的专利申请情况，以监控竞争对手的研发活动。如果检索到的竞争对手的专利申请与企业技术方案实质性相同，则可以视情况采取行动。
- 建设和完善企业内部制度，具体包括保密政策、行为准则和信息管理制度等，确保在日常运营过程中，无论是企业内部员工、企业客户、合作方、承包商及供应商等，均受到相关保密义务的约束。
- 为防止员工通过电子手段窃取和泄露商业秘密及其他保密信息，企业可以考虑部署监控软件监控员工的工作电子邮件和互联网的使用情况。但是，对员工的任何监控必须遵守本地数据保护和劳动法的规定。员工必须清楚地被告知他们可能会被监控。在员工入职时，应落实好相关监控政策宣传，并定期进行保密制度培训。

2.6.1.3 发现侵权行为后的维权策略

如果发现第三方涉嫌侵权，企业应当立即采取调查取证措施保存侵权证据，同时寻求法律维权措施，例如包括：发送警告函、行政投诉、民事侵权诉讼等，严重时还可以选择刑事报案。

(1) 调查取证

为了避免侵权人警觉而难以取证，在对侵权人发起维权主张（例如发送警告函）之前，应尽可能地完成前期调查和证据固定工作。

例如，内部员工涉嫌侵犯商业秘密的：

- 如果内部已部署有监控软件，应继续监控该员工的相关操作及数据流向，同时决策是否向该员工发出警告、停职调查或直接予以辞退；
- 考虑没收、封存该员工的电脑或移动硬盘等设备，并对设备的交接和封存过程进行公证保全（如可行）；
- 对封存的设备中的数据进行镜像复制，镜像过程建议公证保全（如可行）；
- 对镜像副本进行数据分析，防止任何不当操作，删除或干扰原数据的存储方式及内容。

企业应从网络资源、产品测试信息、用户手册等中获取证据。在无法从该等来源获取证据的情况下，例如软件版权侵权，应进行详细的源代码分析和反向工程技术收集证据。

(2) 发送警告函

发送警告函是知识产权维权中最为常用的手段之一。发送警告函前，应确保已经对关键侵权证据进行了保全，已做好必要的诉讼或应诉准备；发送警告函后，针对对方的不同反应可以做出如下不同策略安排：

对方的反应	对策
没有反应	尝试通过不同方式联系接收人，争取得到回复。如果最终仍没有回复，则考虑通过诉讼程序要求对方停止侵权。

可能实际侵权，但回复中坚称不侵权	做好充足的诉讼准备；如证据不强，考虑进一步调查取证。
要求提供更多证据	提供更多证据有助于加强己方主张，但同时可能会过早暴露己方策略及证据弱点，需基于证据强弱个案分析。
不承认侵权，但同意改正或考虑协商许可事宜	反映出侵权人认识到了相关风险，且对侵权事宜较为敏感。
承认侵权并积极承诺停止侵权行为	可以要求其签署不侵权声明或向其授予专利许可。
提出确认不侵权之诉	应在发函之初就充分认识到对方具有该项诉权，避免在事实尚不清楚或未完成证据保全工作前贸然发函。同时，应密切关注对方是否发送催告函[12]，并在其发出后尽快提起侵权诉讼以争取管辖权优势。
提出商业诋毁之诉	如果发函对象范围较广，且函件内容不符合客观事实，对方可以针对企业的发函行为提起商业诋毁之诉。

(3) 民事诉讼

侵权方收到警告函，但未停止侵权的，企业可以向有管辖权的中国法院提起民事诉讼；企业也可以选择不发送警告函而直接提起侵权诉讼。起诉时需要提交起诉状、证据目录和证据。

在商业秘密侵权案件中，需要提交充分的证据以证明：(1) 涉案信息构成商业秘密（未被公众所知悉、采取了保密措施、具有价值性/实用性）以及商业秘密载体；(2) 被告具有接触企业商业秘密的可能性；以及 (3) 被告获取、披露、使用、允许他人使用的信息与主张秘密点的技术信息实质性相似。

在起诉前和法院审理案件过程中，企业可以向法院申请行为保全，要求侵权人立即停止侵权行为。如法院采取行为保全措施，通常会持续到案件裁判生效时止。不过，行为保全申请的要求较高，法院很少批准。除此以外，企业还可以向法院申请采取财产保全、证据保全，以防止侵权方提前转移、隐匿财产或毁灭证据。

通过民事诉讼获得的救济措施主要包括停止侵权（禁令）、损害赔偿。

(4) 行政投诉

除民事诉讼外，企业还可以选择向侵权人所在地、侵权行为地的市场监督管理部门发起行政投诉。

监督管理部门认定侵犯商业秘密行为成立的，可责令停止违法行为、没收违法所得、处以罚款。但由于商业秘密侵权案件的审理难度极大，行政机关立案受理的条件较高。

[12] 在企业发出警告函/律师函后，对方可向企业发送催告函，催告企业撤回律师函或提起诉讼，如企业在收到书面催告 1 个月内或书面催告发出后 2 个月内未撤回律师函或提起诉讼，则对方可主动提起确认不侵权之诉。

(5) 刑事报案

针对商业秘密侵权纠纷，企业还可以选择刑事救济途径，除了同样需要有完整的证据链，还需要达到重大损失的立案标准[13]。

2.6.2 侵犯他人商业秘密的风险及应对策略

2.6.2.1 商业秘密侵权风险

在企业雇佣新员工（尤其是在业内具有丰富经验的员工）时，有可能由于新员工不当地将原雇主的商业秘密信息引入到企业的日常运营中，进而导致商业秘密侵权纠纷。例如，新员工向企业共享竞争对手（原雇主）的客户名单、员工名单、供应商名单、定价、库存信息、专有技术等；竞争对手的公司业务流程；竞争对手对新产品、流程、系统的研究等。

2.6.2.2 预防侵犯他人商业秘密的风险控制措施

预防侵犯他人商业秘密的风险控制措施包括：

(1) 梳理清楚员工拟使用、提供的商业秘密的权利归属并确保员工遵守本指引的规定：
- 在新员工入职程序中要求其提供与前雇主签署的关于知识产权归属的协议，说明在前雇主所担任的工作职责；
- 要求员工签署书面形式的协议或声明，承诺保证不侵犯他人知识产权、不拥有他人的知识产权、不会在任职过程中使用他人的知识产权。

(2) 确保合作方，如其他同业公司、承包商、客户、高校、研究院、初创型企业、大型科技企业等，及其员工遵守本指引的规定。要求合作方签署书面协议或声明，承诺不侵犯他人的知识产权、不拥有他人的知识产权、不会在合作过程中不侵犯他人的知识产权。

(3) 采购合同中约定不侵权保证条款，要求对方承诺其提供的产品或技术不会侵犯第三方知识产权，且一旦发生侵权纠纷将赔偿企业因此遭受的损失。此外，应妥善保管采购协议、发票等凭证，以便在发生涉及产品的侵权纠纷时用以证明该产品拥有合法来源，从而可能免除赔偿责任。

(4) 建立完善的知识产权评估和管理制度，及时将生产经营中产生的技术成果纳入企业的知识产权保护体系，从而防御他人率先取得权利并向企业主张权利。

(5) 定期审查企业的知识产权组合可以确保与企业的总体战略保持一致，并有助于避免

[13] 参见前引 5。

可能不再重要的知识产权相关成本。

(6) 对可能的侵权证据进行管控。在诉讼中，书面沟通记录更容易被权利人作为证据提交。因此，在处理疑似侵权事宜，包括企业可能侵犯他人商业秘密或者他人主张企业侵权时，应尽量通过口头形式沟通。如通过电子邮件、即时通讯等书面形式沟通时，应避免使用“侵权”、“无效”以及第三方专利是否适应于特定场景的表述，同时应避免指明特定的产品、专利号等信息。

2.6.2.3 对他人侵权主张的应对策略

他人针对企业提起侵权主张的情形可能包括：侵权警告函、行政投诉、以及民事诉讼、刑事举报。面对不同情形的侵权主张，在确认具体行动方案之前，均需要完成事实确认和证据固定等事宜。如果企业收到他人的侵权警告函，应当：

(1) 确认发函人主张的商业秘密；
(2) 查明其指控的侵权产品、服务以及具体侵权行为；
(3) 保留所有往来函件（包括信封）以及与被指控行为相关的文件；
(4) 及时咨询外部律师，确认如下事项：
- 发函人所主张的商业秘密是否有效；
- 被指控的侵权行为的范围及程度；
- 企业内部应采取哪些行动来应对对方的侵权主张；
- 对方提起诉讼的可能性及带来的风险；
- 其他必须或者建议采取的行动。

(5) 在完成以上各项的基础上，确认应对侵权警告函的行动方案，企业可以采取的行动包括：
- 回复警告函；
- 提起反制诉讼，例如确认不侵权之诉、商业诋毁之诉、专利侵权之诉；
- 根据实际情况，与对方达成和解。

如果权利人对企业提起行政投诉、民事侵权诉讼或刑事举报，应第一时间通知并委派专业律师参与到相应程序中，包括：

(1) 向律师提供所有法律文件（例如对方提交的起诉状、证据目录、证据、行政投诉书等）；
(2) 核实并确认原告主张的涉嫌侵权行为，并保留所有相关文件；
(3) 与律师沟通，确定如下事项：
- 对方侵权主张成立的可能性；
- 针对对方主张确定抗辩理由；
- 围绕确定的抗辩理由，调查、收集并保全反驳证据；
- 梳理反驳证据，并确定需要保密审理的相关证据内容；
- 程序上如何处理，是否需要拖延诉讼程序为证据搜集等事宜争取时间；
- 对方主张的权利基础是否有瑕疵。

(4) 在此基础上，企业可以考虑采取如下措施：
- 与对方协商、和解；

- 针对对方主张的权利基础的有效性提出质疑；
- 进行充分准备，确定抗辩理由，积极应诉；
- 提起反制诉讼。

需要注意的是，不论最终确定的整体行动方案如何，均应在尽可能完善上述各项准备工作的基础上开展，以保证后续策略选择的灵活性。在此基础上，若企业经过分析，认为存在较大的侵权风险，可以考虑对产品、技术进行规避设计，并可以与对方接触，探讨和解的可行性。若经分析发现并不侵权，则并非必须进行规避设计、和解。此时，可以考虑回复律师函向对方明确表明不侵权、积极应诉或提起商业诋毁之诉等反制措施。

第三部分 商业秘密数据保护解决方案

3.1 计算基础设施和平台服务

3.1.1 本地数据中心建设（配电、温湿度、监控、门禁、消防、机房进出人员管理）

数据中心是企业的核心部分，它为企业提供了计算、存储、网络等基础设施。为了确保数据中心的安全和稳定运行，需要关注以下几个方面：

a) 机房配电：数据中心需要稳定、可靠的电源供应。应确保供电系统具有足够的容量，以满足设备的正常运行需求。此外，还需提供备用电源，如 UPS（不间断电源）和柴油发电机，以应对突发的电源中断情况。

b) 机房温湿度控制：机房内部的温度和湿度对设备的运行和寿命有很大影响。建议将温度控制在 18-27 摄氏度，相对湿度控制在 40%-60%之间。为此，可以采用空调、风扇等设备进行调节，并定期检查与维护。

c) 机房监控：数据中心需要 24 小时不间断的视频监控，以确保设备和数据的安全。监控系统应具有报警功能，一旦发生异常情况，可以及时通知相关人员进行处理。

d) 门禁管理：通过设置门禁系统来限制人员进出数据中心。只有经过授权的人员才能进入机房，以降低数据泄露和设备损坏的风险。同时，要记录每个人的进出时间和目的，以便追踪和审计。

e) 消防设施：数据中心应配备灭火器、自动喷水灭火系统、烟雾探测器等消防设备，并定期进行检查和维护。此外，应定期组织消防演练，提高员工的消防安全意识和应对能力。

f) 机房进出人员管理：对于进出机房的人员，应实行严格的管理制度。包括对员工进行背景调查、签订保密协议、定期培训等措施，以确保数据中心的安全和稳定运行。

3.1.2 计算服务器管理（物理机、虚拟机、超融合）

计算服务器是数据中心的核心组成部分，提供了大量的计算资源。有效管理计算服务器可以确保业务的高效运行和数据安全。针对不同类型的服务器，如物理机、虚拟机和超融合服务器，管理策略略有不同：

a) 物理机管理：

资产管理：对物理服务器进行编号和标签，建立资产管理系统，记录服务器的配置、位置、使用状态等信息，便于维护和故障排查。

系统安装与配置：为服务器安装合适的操作系统和软件，进行必要的网络和安全配置。定期检查系统更新，确保运行环境的安全和稳定。

监控与维护：实施实时监控，关注服务器的 CPU、内存、磁盘、网络等关键指标。发现问题时及时处理，定期进行硬件检查和维护。

b) 虚拟机管理：

虚拟机创建与配置：根据业务需求创建适量的虚拟机，为其分配合适的资源（如 CPU、内存、磁盘等），并进行操作系统和软件安装。

虚拟机监控与维护：监控虚拟机的运行状态和资源使用情况，确保其正常运行。对于故障虚拟机，进行故障排查和恢复。同时，定期对虚拟机进行备份和系统更新。

资源调整与优化：根据业务变化和资源使用情况，对虚拟机进行动态资源调整，提高资源利用率。在必要时，可以实施虚拟机迁移，以优化资源分布。

c) 超融合服务器管理：

集群管理：超融合服务器通常部署在集群环境中。需要监控集群的整体性能和运行状态，发现问题时及时处理。同时，根据业务需求，可以对集群进行扩容或缩容。

资源分配与优化：在超融合环境下，计算、存储和网络资源被统一管理。需要合理分配资源给各个业务，确保资源的高效利用。通过监控和分析，可以发现并解决资源瓶颈问题。

数据保护与恢复：超融合服务器存储了大量重要数据。需要定期进行数据备份，并建立灾备机制，以应对突发事件。在数据丢失或损坏时，能够迅速恢复数据，确保业务的连续性。

3.1.3 SaaS 平台管理（平台数据备份）

SaaS（Software as a Service，软件即服务）是一种将软件以服务的形式提供给用户的模式。SaaS 平台管理的重点之一是确保平台数据的安全和完整。为此，需要建立合适的数据备份策略和流程，以下是一些建议：

a) 定期备份：根据业务需求和数据价值，设定合适的备份周期（如每日、每周、每月等），并定期执行备份任务。可以使用自动化工具和脚本进行备份，以提高效率和准确性。

b) 多级备份：实施多级备份策略，如完全备份、增量备份和差异备份。完全备份即备份所有数据，增量备份和差异备份则只备份上次备份后发生变化的数据。多级备份可以降低备份所需的存储空间和时间成本。

c) 离线与异地备份：为防止数据中心发生灾难性事件（如火灾、洪水等），建议进行离线和异地备份。离线备份指将数据备份到脱机介质，如磁带或可移动硬盘；异地备份则是将数据备份到另一地理位置的数据中心。

d) 数据加密：对于敏感和重要数据，应在备份过程中进行加密，以保护数据的安全和隐私。加密算法应选择经过广泛验证的标准算法，如 AES（Advanced Encryption Standard）。

e) 测试与验证：定期对备份数据进行测试和验证，以确保备份的可用性和完整性。测试可以包括恢复部分或全部数据，以验证数据的一致性和完整性。

f) 备份监控与报告：对备份过程进行监控，记录备份任务的执行情况和结果。发现问题时及时进行处理。定期生成备份报告，以供审计和管理分析。

通过有效的 SaaS 平台数据备份管理，可以确保业务连续性，降低数据丢失和损坏的风险，为用户提供更加稳定和可靠的服务。

3.1.4 PaaS 平台管理（平台数据安全和备份）

PaaS（Platform as a Service，平台即服务）是一种提供应用程序运行和开发环境的云服务模式。在管理 PaaS 平台时，数据安全和备份是关键因素。以下是一些建议和策略：

a) 访问控制：实施严格的访问控制策略，确保只有授权用户才能访问 PaaS 平台上的敏感数据和资源。使用身份认证和授权机制，如 OAuth 2.0、SAML（安全断言标记语言）等，对用户进行身份验证。

b) 数据加密：对存储和传输中的数据进行加密，以保护数据的安全和隐私。对于存储数据，使用透明数据加密（TDE）等技术进行加密；对于传输数据，使用 SSL/TLS 等协议进行加密。

c) 安全监控：实施实时安全监控，检测并防范潜在的安全威胁。使用入侵检测系统（IDS）和入侵防御系统（IPS）等工具，识别和阻止恶意行为。

d) 定期备份：根据业务需求和数据价值，设置合适的备份周期（如每日、每周、每月等），并定期执行备份任务。可以使用自动化工具和脚本进行备份，以提高效率和准确性。

e) 多级备份：采用多级备份策略，如完全备份、增量备份和差异备份。这样可以降低备份所需的存储空间和时间成本，同时确保数据的完整性。

f) 离线与异地备份：进行离线和异地备份，以防止数据中心发生灾难性事件（如火灾、洪水等）。离线备份是将数据备份到脱机介质，如磁带或可移动硬盘；异地备份则是将数据备份到另一地理位置的数据中心。

g) 测试与验证：定期对备份数据进行测试和验证，以确保备份的可用性和完整性。测试可以包括恢复部分或全部数据，以验证数据的一致性和完整性。

h) 备份监控与报告：对备份过程进行监控，记录备份任务的执行情况和结果。发现问题时及时进行处理。定期生成备份报告，以供审计和管理分析。

通过实施这些策略，可以确保 PaaS 平台的数据安全和稳定运行，为用户提供可靠的开发和运行环境。

3.1.5 混合云平台管理（私有云和公有云、多云管理）

混合云是将私有云和公有云结合起来的一种云计算模式，可以实现资源的优化分配和管理。在混合云平台管理中，需要注意以下几个方面：

a) 统一管理平台：为了简化混合云环境的管理，可以使用统一的管理平台，实现对私有云和公有云资源的集中管理和监控。

b) 数据安全与隐私：在混合云环境中，数据在私有云和公有云之间传输和存储，需要特别关注数据安全和隐私。实施加密、访问控制和安全监控等措施，以保护数据的安全和隐私。

c) 负载均衡与弹性伸缩：在混合云环境中，可以根据业务需求和资源使用情况，灵活调整负载分配和资源分配。使用负载均衡器、弹性伸缩组等技术，实现自动化的资源调整和优化。

d) 跨云备份与恢复：在混合云环境中，可以利用不同云之间的资源，实现跨云备份和恢复。例如，将私有云中的数据备份到公有云，或者在多个公有云之间进行数据备份，以提高数据的可靠性和可用性。

e) 网络优化：为了确保混合云环境中的网络性能和稳定性，需要对网络进行优化。使用 VPN（虚拟专用网络）、SD-WAN（软件定义广域网）等技术，实现安全、高效的网络连接。

f) 混合云策略与治理：制定合适的混合云策略，明确私有云和公有云的使用范围和目的。建立统一的治理框架，包括成本管理、性能监控、安全策略等，以确保混合云环境的有效管理。

g) 多云管理：在多云环境中，可能会使用多个公有云提供商。需要关注不同云平台之间的兼容性和互操作性，并采用适当的多云管理工具，实现对多个云平台的统一管理和监控。

通过以上措施，可以实现混合云平台的有效管理，降低管理复杂性，提高资源利用率和业务连续性。

3.2 网络

3.2.1 基础网络管理（防火墙、交换机、无线 AC、AP、综合布线）

基础网络管理涉及到组织内部的各种网络设备和技术的配置、监控和维护。以下是针对不同设备和技术的网络管理要点：

a) 防火墙管理：

规划合理的网络拓扑，确保内外网隔离，降低安全风险。

设定合适的安全策略，包括访问控制列表（ACL）、端口过滤等，阻止非法访问和攻击。

定期更新防火墙规则和软件，保持安全防护能力的最新状态。

监控防火墙日志，分析和处理异常事件。

b) 交换机管理：

合理规划交换机的位置和连接方式，保证网络性能和稳定性。

配置 VLAN（虚拟局域网）以实现网络隔离，降低广播风暴和安全风险。

启用端口安全特性，如 BPDU（网桥协议数据单元）保护、端口速率限制等，防止攻击和滥用。

监控交换机的状态和性能，如 CPU 利用率、内存利用率、端口流量等，及时发现和处理问题。

c) 无线 AC（接入控制器）管理：

合理布局无线接入控制器，保证覆盖范围和信号质量。

配置合适的无线频段和信道，避免信道干扰和性能下降。

启用无线安全特性，如 WPA（Wi-Fi Protected Access）加密、客户端隔离等，保护用户数据和隐私。

监控无线 AC 的状态和性能，如连接用户数、信道利用率等，及时发现和处理问题。

d) AP（接入点）管理：

合理布局 AP，确保无线信号覆盖范围和质量。

与无线 AC 配合，实现无缝漫游和负载均衡。

监控 AP 的状态和性能，如信号强度、连接用户数等，及时发现和处理问题。

e) 综合布线管理：

规划合理的布线路径和方式，避免干扰和损耗。

使用合格的布线材料和设备，如光纤、双绞线、配线架等，保证网络性能和稳定性。

对布线进行标准化、规范化的管理，如线缆标签、线缆管理器等，方便维护。

网络流量分析（上网行为管理、内网接入管理）

网络流量分析对于维护网络安全、提升网络性能和确保合规性具有重要意义。主要包括上网行为管理和内网接入管理两个方面：

a) 上网行为管理：

内容过滤：使用内容过滤系统，对上网行为进行监控和限制，阻止访问包含恶意软件、钓鱼网站或不符合企业政策的网站。

应用控制：通过应用层防火墙或其他网络设备，识别并控制网络中的各种应用程序流量，如即时通讯、文件传输、社交媒体等。

带宽管理：对网络流量进行分析，确保关键业务系统具有足够的带宽资源。通过限速、优先级控制等手段，对非关键业务流量进行限制。

用户行为审计：记录并分析用户上网行为，确保遵循企业政策和合规要求。对异常或违规行为进行预警和处理。

b) 内网接入管理：

身份认证：对接入内网的设备和用户进行身份认证，确保只有授权用户才能访问网络资源。使用 802.1X、RADIUS 等技术实现强身份认证。

网络准入控制：通过网络准入控制（NAC）系统，对接入设备进行安全检查，如操作系统补丁、防病毒软件、系统配置等。只有满足安全要求的设备才能接入网络。

角色权限分配：根据用户角色和权限，限制对网络资源和服务的访问。使用访问控制列表（ACL）、虚拟局域网（VLAN）等技术实现访问控制。

内部网络监控：持续监控内网流量，通过网络流量分析工具（如 NetFlow、sFlow 等）实时发现和处理异常流量、攻击行为等。

通过上网行为管理和内网接入管理，企业可以确保网络的安全性、稳定性和合规性，提高网络资源利用率，保障关键业务系统的正常运行。

3.2.2 企业网络管理（物理隔离、逻辑隔离，ACL 访问控制）

企业网络管理需要综合考虑安全性、稳定性和可扩展性。物理隔离、逻辑隔离和访问控制是实现这一目标的关键技术。

a) 物理隔离：

对关键网络设备和服务器进行独立部署，防止因设备共享导致的安全风险。

使用独立的网络设备和线路连接不同安全级别的网络，确保敏感数据不会泄露。

在机房内采用物理隔离手段，如不同区域的机柜设置门禁，防止未经授权的人员接触关键设备。

b) 逻辑隔离：

使用虚拟局域网（VLAN）技术，将网络按照功能、安全级别等划分为多个逻辑子网，限制广播域和非法访问。

在路由器和防火墙上配置虚拟路由和转发（VRF）实例，实现不同网络之间的逻辑隔离。

使用软件定义网络（SDN）技术，灵活管理网络资源，实现动态的网络隔离和划分。

c) ACL 访问控制：

在网络设备（如路由器、交换机、防火墙等）上配置访问控制列表（ACL），限制不同设备和用户对网络资源的访问。

根据用户角色和权限，设定合适的访问策略，实现对敏感数据和关键服务的保护。

定期审查和更新 ACL 规则，确保访问控制策略与企业安全政策保持一致。

通过物理隔离、逻辑隔离和 ACL 访问控制技术，企业可以构建安全、稳定和易于管理的网络环境，满足不同业务需求和合规要求。同时，还需要定期对网络设备和配置进行审查和更新，以应对新的安全挑战和业务变化。

3.2.3 企业多分支组网管理（ 点对点 VPN、SD-WAN、远程办公零信任访问）

企业多分支组网管理需要确保各分支网络之间的高效、安全和可靠连接。点对点 VPN、SD-WAN 和远程办公零信任访问是实现这一目标的关键技术。

a) 点对点 VPN（Virtual Private Network）：

通过在公共网络上创建加密隧道，实现分支间的安全通信，保障数据传输的机密性、完整性和可用性。

配置合适的加密算法和认证机制，提高 VPN 连接的安全性。

监控 VPN 连接状态，确保网络连通性和性能。

b) SD-WAN（Software-Defined Wide Area Network）：

利用软件定义网络（SDN）技术，动态管理企业的广域网资源，实现分支间的智能路由和优化。

集中管理网络策略，简化网络配置和维护工作。

支持多种接入方式（如 MPLS、Internet、4G/5G 等），提高网络连接的灵活性和可靠性。

提供端到端的网络质量监控和优化，确保关键业务系统的性能和稳定性。

c) 远程办公零信任访问：

采用零信任网络访问（ZTNA）策略，对所有远程办公用户进行身份验证和设备检查，确保只有合规设备和授权用户才能访问企业资源。

使用微段网络（Micro-segmentation）技术，对远程办公用户的访问权限进行细粒度控制，限制对敏感数据和关键服务的访问。

监控远程办公用户的行为和网络状态，及时发现并处理安全威胁和异常事件。

通过点对点 VPN、SD-WAN 和远程办公零信任访问技术，企业可以构建安全、高效和易于管理的多分支组网环境，满足不同业务需求和合规要求。同时，还需要定期对网络设备和配置进行审查和更新，以应对新的安全挑战和业务变化。

3.3 安全

3.3.1 网络安全（防火墙 IPS、WAF、日志审计）

网络安全对于保障企业数据、业务和声誉至关重要。以下是针对防火墙 IPS、WAF 和日志审计的网络安全管理要点：

a) 防火墙 IPS（Intrusion Prevention System）：

防火墙 IPS 作为主动防御系统，可以实时监控网络流量，识别并阻止潜在的恶意活动和攻击。

定期更新 IPS 规则和签名库，以应对新的安全威胁和漏洞。

对 IPS 进行性能监控和故障排查，确保其稳定运行，不影响网络性能。

结合其他安全设备和策略，构建多层次的防御体系。

b) WAF（Web Application Firewall）：

WAF 针对 Web 应用程序提供安全保护，防止 SQL 注入、跨站脚本（XSS）、跨站请求伪造（CSRF）等攻击。

根据企业 Web 应用的特点，定制 WAF 规则和策略，提高安全防护效果。

监控 WAF 的性能和状态，确保其正常运行，不影响业务系统的可用性。

定期审查和更新 WAF 配置，以适应业务变化和新的安全需求。

c) 日志审计：

对网络设备（如防火墙、IPS、WAF 等）和业务系统产生的日志进行收集、归档和分析，以监控网络状态和安全状况。

使用日志管理和分析工具（如 SIEM 系统），实现日志的自动处理和实时告警，提高安全事件响应速度。

遵循企业政策和法律法规要求，对日志数据进行加密存储、访问控制和数据保留。

定期对日志审计工作进行审查和改进，提高安全监控能力。

通过实施防火墙 IPS、WAF 和日志审计策略，企业可以建立有效的网络安全防护体系，及时发现和处理安全威胁，保障业务的正常运行。同时，需要定期评估网络安全状况和策略有效性，以应对不断变化的安全挑战。

3.3.2 服务器主机安全（主机安全防护软件、操作系统补丁管理）

保障服务器主机安全是网络安全的重要组成部分，需要采取多种措施来提高服务器主机的安全性，包括主机安全防护软件和操作系统补丁管理。

a) 主机安全防护软件：

安装并维护有效的防病毒软件，定期更新病毒库，以防止恶意软件的感染。

部署主机入侵检测和防护系统（HIDS/HIPS），实时监控服务器的行为和状态，发现并阻止潜在的攻击和入侵。

使用系统漏洞扫描工具，定期检查服务器的安全漏洞和配置问题。

对服务器文件和数据进行加密，保障数据的机密性和完整性。

b) 操作系统补丁管理：

关注操作系统厂商的安全公告和补丁发布，及时获取关于已知漏洞和补丁的信息。

根据企业的安全策略和业务需求，制定补丁管理流程和策略，包括补丁测试、验证和部署。

定期对服务器进行操作系统补丁更新，修复已知漏洞，防止攻击者利用漏洞进行攻击。

针对关键服务器和业务系统，采取额外的安全措施，如隔离、加固和访问控制，降低安全风险。

通过实施主机安全防护软件和操作系统补丁管理策略,企业可以有效提高服务器主机的安全性，防止恶意软件感染和攻击者入侵。同时，需要定期评估服务器主机的安全状况和策略有效性，以应对不断变化的安全挑战。

3.3.3 终端安全（终端账号权限、终端防病毒软件、终端数据备份、数据防泄漏）

终端安全是企业网络安全的重要组成部分，需要从多个方面来保障终端设备的安全性，包括终端账号权限、终端防病毒软件、终端数据备份和数据防泄漏。

a) 终端账号权限：
为每个用户分配独立的账号，实现身份识别和访问控制。
根据用户的职责和业务需求，设置合适的账号权限，避免权限过大导致的安全风险。
定期审查用户账号和权限，删除不再使用的账号，调整权限设置。
对用户进行安全培训，提高用户对账号安全和密码管理的认识。

b) 终端防病毒软件：
在所有终端设备上安装并维护防病毒软件，定期更新病毒库，以防止恶意软件的感染。
配置防病毒软件的实时扫描和定时扫描功能，确保持续的安全防护。
监控终端设备的安全状态，及时处理恶意软件感染和其他安全事件。

c) 终端数据备份：
制定终端数据备份策略和计划，包括备份范围、时间和周期。
使用可靠的备份工具和存储介质，保障备份数据的完整性和可用性。
对备份数据进行加密和访问控制，防止数据泄露和恶意篡改。
定期验证备份数据的可恢复性，确保数据备份的有效性。

d) 数据防泄漏：
部署数据泄露防护（DLP）系统，监控和控制敏感数据的存储、传输和使用。
对敏感数据进行加密，防止未经授权的访问和泄露。
对员工进行数据安全培训，提高员工对数据保密和安全使用的认识。
定期审查数据防泄漏策略和措施，以应对新的安全挑战和业务需求。

通过实施终端账号权限、终端防病毒软件、终端数据备份和数据防泄漏策略，企业可以有效保障终端设备的安全性，防止数据泄露和恶意攻击。同时，需要定期评估终端安全状况和策略有效性，以应对不断变化的安全挑战。

3.3.4 应用安全（共享文档、OA、ERP、CRM、企业邮件系统等系统、数据安全、代码安全、反垃圾邮件）

应用安全是企业信息安全的关键组成部分，涉及多个方面，如共享文档、OA、ERP、CRM、企业邮件系统等业务系统的安全、数据安全、代码安全，以及反垃圾邮件等。

a) 业务系统安全：

对企业内部的业务系统（如共享文档、OA、ERP、CRM 等）实施统一的安全管理，确保系统符合企业安全策略。

部署防火墙、入侵检测和防护系统（IDS/IPS）、Web 应用防火墙（WAF）等安全设备，保护业务系统免受攻击。

定期进行系统漏洞扫描和安全评估，修复已知的安全漏洞。

对业务系统的访问和操作实施访问控制、身份认证和权限管理。

b) 数据安全：

对敏感数据进行加密，防止数据泄露和未经授权的访问。

部署数据泄露防护（DLP）系统，监控和控制敏感数据的存储、传输和使用。

制定数据备份策略，定期备份关键数据，以确保数据的完整性和可恢复性。

c) 代码安全：

在软件开发过程中遵循安全编程规范，防止安全漏洞的产生。

对开发人员进行安全培训，提高安全意识和编程规范性。

使用代码审查工具和静态应用程序安全测试（SAST）工具，检查代码中的安全问题。

对已发布的应用程序进行动态应用程序安全测试（DAST），发现潜在的安全漏洞和风险。

d) 企业邮件系统安全：

部署邮件网关和防病毒软件，对收发邮件进行安全检查，防止恶意软件和钓鱼邮件的传播。

使用反垃圾邮件技术，过滤垃圾邮件，减轻员工和系统的负担。

对企业邮件系统进行访问控制和身份认证，防止未经授权的访问和操作。

对企业邮件中的敏感数据进行加密和保护，防止数据泄露。

通过实施上述应用安全措施，企业可以有效保护关键业务系统和数据，防止安全漏洞和攻击。同时，需要定期评估应用安全状况和策略有效性，以应对不断变化的安全挑战。

3.3.5 身份认证管理（统一身份认证（SSO）、账号权限管理、密码管理）

身份认证管理是企业信息安全的重要组成部分，主要包括统一身份认证（SSO）、账号权限管理和密码管理。通过实施有效的身份认证管理策略，企业可以确保只有合法用户才能访问和操作敏感数据和系统。

a) 统一身份认证（SSO）：

部署单点登录（SSO）解决方案，使用户只需登录一次就可以访问企业内部的多个业务系统。

通过 SSO 简化用户认证过程，提高用户体验，降低密码管理的复杂性。

与多因素认证（MFA）技术结合，增强身份认证的安全性。

b) 账号权限管理：

为每个用户分配独立的账号，实现身份识别和访问控制。

根据用户的职责和业务需求，设置合适的账号权限，避免权限过大导致的安全风险。

定期审查用户账号和权限，删除不再使用的账号，调整权限设置。

对用户进行安全培训，提高用户对账号安全和权限管理的认识。

c) 密码管理：

制定密码策略，要求用户设置复杂度较高的密码，降低密码被破解的风险。

要求用户定期更换密码，避免长时间使用相同的密码导致的安全隐患。

提醒用户不要在多个系统或应用中使用相同的密码。

使用密码管理工具，帮助用户安全地存储和管理密码。

通过实施统一身份认证（SSO）、账号权限管理和密码管理策略，企业可以有效保障用户身份的安全性，降低数据泄露和恶意攻击的风险。同时，需要定期评估身份认证管理状况和策略有效性，以应对不断变化的安全挑战。

3.3.6 安全培训和意识（提高开发人员、运维人员和使用人员的安全意识，让他们了解应用安全的重要性和最佳实践）

安全培训和意识是确保企业信息安全的基石。通过提高开发人员、运维人员和使用人员的安全意识，让他们了解应用安全的重要性和最佳实践，可以有效地降低安全风险。以下是一些建议：

a) 制定安全培训计划：

根据员工的职责和需求，为不同角色的员工制定合适的安全培训计划。

定期更新培训内容，确保培训计划与安全形势和技术发展保持同步。

b) 采用多种培训形式：

结合线上和线下的培训形式，提高培训的灵活性和效果。

采用案例分析、模拟演练、实战演练等多种培训方法，帮助员工更好地理解和掌握安全知识和技能。

c) 评估培训效果：
通过测试、考核和评估，了解员工的安全培训效果。
根据评估结果，调整培训计划和内容，提高培训质量。

d) 建立安全文化：
在企业内部宣传安全意识，强调安全对于企业成功的重要性。
鼓励员工积极参与安全活动，提高安全意识。
为员工提供安全资源和支持，帮助他们解决安全问题。

e) 激励和奖励：
对在安全培训和实践中表现出色的员工给予表彰和奖励。
将安全表现纳入员工绩效考核，强化安全意识在企业文化中的地位。

通过实施有效的安全培训和意识计划，企业可以提高员工的安全素养，降低安全风险。同时，需要定期评估培训和意识计划的效果，并根据实际情况调整和优化，以应对不断变化的安全挑战。

3.4 存储和数据库

3.4.1 数据备份和恢复（数据备份类型结构化或非结构化、备份存储介质、数据恢复的 RTO 和 RPO）

数据备份和恢复是确保企业业务连续性和数据安全的重要措施。根据数据类型（结构化或非结构化）、备份存储介质以及数据恢复的时间目标（RTO）和数据点目标（RPO），企业可以制定合适的数据备份和恢复策略。

a) 数据备份类型：
结构化数据：通常存储在关系数据库中，如客户信息、订单记录等。备份结构化数据时，需要考虑如何最大程度地减少业务系统的性能影响。
非结构化数据：包括文档、图片、视频等多种格式的文件。备份非结构化数据时，需要考虑如何确保数据的完整性和可用性。

b) 备份存储介质：
磁盘备份：利用磁盘阵列或独立磁盘进行数据备份，具有较高的读写速度，便于数据恢复。但磁盘备份成本较高，且易受物理损坏影响。
磁带备份：采用磁带存储备份数据，具有较低的成本和较长的数据保留期。但磁带备份速度较慢，且恢复数据时可能需要较长时间。
云备份：将数据备份至云存储服务，具有较高的可扩展性和灵活性。云备份可以实现地理冗余，降低因自然灾害等原因导致的数据丢失风险。

c) 数据恢复的 RTO 和 RPO：

恢复时间目标（RTO）：指数据恢复所需的最大时间。根据业务需求，企业需要确定合适的 RTO，以确保业务在可接受的时间内恢复正常。

恢复点目标（RPO）：指在数据丢失或损坏后，可以接受的数据丢失的最大时间。企业应根据业务要求和容忍度，设定合适的 RPO，并根据 RPO 制定相应的备份策略。

通过综合考虑数据类型、备份存储介质以及数据恢复的 RTO 和 RPO，企业可以制定有效的数据备份和恢复策略，确保业务连续性和数据安全。同时，需要定期评估备份和恢复策略的有效性，以应对不断变化的业务需求和安全挑战。

3.4.2 数据库审计（数据库的增改删、数据库脱敏）

数据库审计是对数据库操作进行监控和记录的过程，主要用于确保数据安全和合规性。数据库审计通常包括对数据增改删操作的监控以及数据库脱敏等措施。

a) 监控数据库的增改删操作：

记录数据库操作日志，包括对数据表的增加、修改和删除操作，以及对数据行的增加、修改和删除操作。

审计日志应包括操作类型、操作时间、操作人、受影响的数据表和数据行等详细信息。

定期分析审计日志，检查是否存在异常操作或潜在的安全风险，如未授权访问、数据泄露等。

b) 数据库脱敏：

对敏感数据进行脱敏处理，以防止数据泄露。常见的脱敏方法包括数据掩码、数据替换、数据加密等。

数据掩码：用特定字符替换敏感数据的部分内容，如将手机号的中间四位替换为“****”。

数据替换：用无关数据替换敏感数据，如将真实姓名替换为化名。

数据加密：对敏感数据进行加密处理，只有拥有密钥的用户才能解密和访问数据。

通过实施数据库审计和脱敏策略，企业可以有效保障数据安全和合规性。同时，需要定期评估数据库审计和脱敏策略的有效性，并根据实际情况调整和优化，以应对不断变化的安全挑战和合规要求。

3.4.3 数据容灾（数据中心、应用异地容灾）

数据容灾是确保企业在面临灾难性事件（如火灾、地震、洪水等）时，能够迅速恢复业务和数据的关键措施。数据容灾通常包括数据中心容灾和应用异地容灾两个方面。

a) 数据中心容灾：

设立异地数据中心：在地理位置分离的地区建立备份数据中心，以降低因自然灾害等原因导致的数据丢失风险。

数据同步与备份：定期将主数据中心的数据同步或备份到异地数据中心，以确保数据的一致性和完整性。

网络冗余：建立多条网络连接线路，确保在某些网络故障时，数据中心之间的通信不受影响。

容灾演练：定期进行数据中心容灾演练，验证数据中心切换和恢复的可行性和效果。

b) 应用异地容灾：

应用程序部署：在主数据中心和异地数据中心部署相同的应用程序，确保在主数据中心出现问题时，可以迅速切换到异地数据中心继续提供服务。

负载均衡与故障切换：利用负载均衡技术，在主数据中心和异地数据中心之间分配用户请求，实现故障切换和业务连续性。

监控与告警：实时监控应用程序的运行状况，发现异常情况时及时发出告警，以便及时采取应对措施。

异地容灾演练：定期进行应用异地容灾演练，验证应用切换和恢复的可行性和效果。

通过实施数据中心容灾和应用异地容灾策略，企业可以有效确保业务连续性和数据安全。同时，需要定期评估容灾策略的有效性，并根据实际情况调整和优化，以应对不断变化的业务需求和安全挑战。

3.5 IT 自动化

3.5.1 应用性能监控 APM（服务器网络、数据库等性能监控）

应用性能监控（APM，Application Performance Monitoring）是一种对应用程序性能进行监测、管理和优化的技术。APM 可以帮助企业发现潜在的性能瓶颈、故障点和异常行为，从而提高应用程序的稳定性和用户体验。APM 通常包括对服务器网络、数据库等关键组件的性能监控。

a) 服务器网络性能监控：

监控服务器的 CPU 使用率、内存使用率、磁盘使用率和网络带宽等关键指标，以了解服务器是否正常运行和是否存在性能瓶颈。

对服务器日志进行实时分析，发现异常事件和潜在的安全风险。

根据监控数据，调整服务器资源配置，优化负载均衡策略，提高服务器性能。

b) 数据库性能监控：

监控数据库的响应时间、连接数、锁等待时间等关键指标，以了解数据库是否正常运行和是否存在性能瓶颈。

对数据库查询进行优化，降低查询响应时间，提高数据库性能。

定期进行数据库维护，如重建索引、更新统计信息等，确保数据库运行效率。

c) 其他组件性能监控：

对应用程序的其他关键组件（如消息队列、缓存服务器等）进行性能监控，以确保整个应用系统的稳定运行。

实时收集并分析组件日志，发现异常行为和潜在的故障点。

通过实施应用性能监控策略，企业可以有效提升应用程序的稳定性、性能和用户体验。同时，需要定期评估 APM 策略的有效性，并根据实际情况调整和优化，以应对不断变化的业务需求和技术挑战。

3.5.2 IT 服务管理 ITSM

IT 服务管理（ITSM，IT Service Management）是一种以 IT 服务为核心的管理方法，旨在通过规范的流程、技术和人员管理，为企业提供高质量、高可靠性的 IT 服务。ITSM 可以帮助企业提高 IT 服务的效率、透明度和响应速度，同时还能够降低 IT 服务的风险和成本。

ITSM 通常包括以下几个方面：

a) 服务目录和服务级别协议（SLA）管理：

建立服务目录，明确 IT 服务的范围、内容和细节，以便用户了解和选择适合自己的服务。

签订服务级别协议（SLA），明确 IT 服务的质量、响应时间和支持方式，以确保用户对服务有清晰的期望和要求。

b) 故障管理：

建立故障处理流程，包括故障发现、诊断、处理、解决和关闭等环节。

实时监控故障状态，并及时通知用户和管理人员，以便及时采取应对措施。

对故障进行分类和归档，以便未来对故障进行统计和分析。

c) 变更管理：

建立变更管理流程，包括变更申请、变更评审、变更实施和变更审核等环节。

确保变更过程的可控性和透明度，避免因不当变更导致的业务中断和风险。

d) 问题管理：

建立问题处理流程，包括问题登记、问题诊断、问题解决和问题关闭等环节。

对问题进行分类和归档，以便未来对问题进行统计和分析。

e) 运维管理：

建立运维管理流程，包括资产管理、配置管理、监控管理和容量管理等环节。

实时监控 IT 资源的状态和性能，及时发现和排除故障，以确保系统稳定运行。

通过实施 IT 服务管理策略，企业可以提高 IT 服务的质量和效率，降低 IT 服务的风险和成本。同时，需要定期评估 ITSM 策略的有效性，并根据实际情况调整和优化，以应对不断变化的业务需求和技术挑战。

3.5.3 桌面和移动终端统一管理

桌面和移动终端统一管理是一种综合性的终端管理技术，旨在通过对桌面和移动终端的统一管理，实现对企业所有终端设备的集中控制和安全管理。桌面和移动终端统一管理通常包括以下几个方面：

a) 设备管理：
对终端设备进行注册和管理，包括设备的基本信息、硬件和软件配置等。
对设备进行分类和分组，以便更好地进行管理和控制。
b) 应用管理：
对终端设备上的应用进行管理和控制，包括应用的安装、升级和卸载等。
对应用进行分类和分组，以便更好地进行管理和控制。

c) 数据管理：
对终端设备上的数据进行管理和控制，包括数据备份、恢复、加密和清除等。
对数据进行分类和分级，以便更好地进行管理和控制。

d) 安全管理：
对终端设备进行安全管理和防护，包括杀毒、防火墙、加密和访问控制等。

第四部分 附录

4.1 商业秘密信息提供登记表

资料或文档名称	技术内容描述	用途	密级	交付时间	归还时间

4.2 员工保密协议

为明确甲方对乙方及关联公司的保密义务,有效保护乙方及关联公司的商业秘密,根据《中华人民共和国民法典》、《中华人民共和国反不正当竞争法》、《中华人民共和国劳动合同法》及有关法律、法规，甲乙双方本着平等、自愿、公平和诚实信用的原则，就甲方在乙方及其关联公司任职、参与乙方及其关联公司工作期间及离职后的保密事项达成如下协议：

第一条　保密信息

为本协议之目的，“**乙方保密信息**”指甲方在乙方工作期间所获取的乙方及/或其关联公司以及合作方所有或知悉的全部信息，无论该等信息以何种形式存在或载于何种载体,也无论甲方得知该等信息的过程中是否以口头或以书面方式被告知其具有保密性，但不包括为公众已普遍知悉的信息。具体而言，乙方保密信息包括但不限于以下几项：

(1)　乙方或其关联公司以及合作方的管理秘密，包括但不限于财务预决算报告及各类财务报表、统计报表等财务资料，人事资料、工资性、劳务性收入、薪酬福利信息、绩效考核信息及资料等工资薪酬资料，物流资料，服务器资料；

(2)　乙方或其关联公司以及合作方的经营秘密，包括但不限于经营方针，投资决策意向，产品服务定价，市场分析，广告策略，研究数据；

(3)　乙方或其关联公司以及合作方的交易秘密，包括但不限于商品产、供、销渠道，客户名单，买卖意向，成交或商谈的价格，商品性能、质量、数量、交货日期，商业合作伙伴的技术信息、资料、数据以及相关业务或事务、经营信息等；

(4)　乙方或其关联公司以及合作方的技术秘密，包括但不限于技术原理、技术思想、技术方案、技术路线、技术工艺、技术细节、技术能力、产品设计、产品图纸、生产模具、作业蓝图、工程设计图、生产制造工艺、制造技术、技术数据科研成果、认证；

(5)　乙方或其关联公司以及合作方所持有的其他与知识产权相关的未公开的信息，包括但不限于未公开或公告的专利、专利申请、商标申请、计算机软件、集成电路布图设计等；

(6)　乙方或其关联公司以及合作方的其他不为公众所知悉，具有商业价值且乙方采取相应保密措施的技术信息、经营信息以及知识产权；

(7)　乙方《商业秘密管理制度》及其他章程、规章规定的信息，或按照乙方商业秘密管理流程评定为商业秘密的其他信息。

第二条　保密义务

2.1　甲方应对因身份、职务、职业或技术关系而知悉的乙方保密信息严格保密，保证不在未取得乙方授权的情况下对外披露或使用，包括意外或过失披露，无论乙方保密信息是否是由甲方因工作而构思或研发所得的。

2.2　甲方在乙方任职期间，必须遵守乙方规定的任何成文或不成文的保密规章、制度（包括但不限于乙方《商业秘密管理制度》），履行与其工作岗位相应的保密职责。乙方的保密规章、制度没有规定或者规定不明确之处，甲方亦应本着谨慎、诚实的态度，采取任何必要、合理的措施，维护其于任职期间知悉或者持有的任何属于乙方或者虽属于第三方但乙方承诺有保密义务的技术、经营秘密或其他商业秘密信息，以保持其秘密性。

2.3　甲方未经授权，不得为下列行为：

(1) 以竞争为目的、或出于私利、或为第三人谋利、或为故意加害于乙方，擅自披露、使用乙方保密信息、制造再现乙方保密信息的器材、取走与乙方保密信息有关的物件；
(2) 刺探与本职工作或本身无关的乙方保密信息；
(3) 直接或间接地向乙方或其关联公司以及合作方内部或外部的无关人员泄露乙方保密信息；
(4) 向不承担保密义务的任何第三人提供乙方保密信息；
(5) 允许（出借、赠予、出租、转让等处分乙方保密信息的行为皆属于“允许”）或协助不承担保密义务的任何第三人使用乙方保密信息；
(6) 复制、下载、再造、复印、分发、传递或以其他方式使用、传播或公开乙方保密信息或将其携带出乙方或其关联公司以及合作方工作场所；
(7) 不正当手段获取保密信息的行为，包括以任何方式使得公司的保密信息脱离公司占有的行为，例如将保密信息发送、上传或以其他方式传输至未经公司许可的邮箱、网盘、服务器、即时通讯工具（包括软件或网页版的微信、QQ 等即时通讯工具）中；通过任何手段使得保密信息存储于未经公司允许的设备中，或通过未经公司允许的设备访问保密信息；未经公司允许的设备包括任何未经公司明确书面许可的外接 USB 存储设备、电脑、笔记本、光盘、平板电脑、手机等存储介质；未经公司允许，制作包含公司保密信息的载体的副本，或将载有公司保密信息的载体或该等载体的副本带离公司。载有公司保密信息的载体包括存储介质、纸质文档、产品本身、样品样机等。本规范所称制作包含公司保密信息的载体的副本，既包括直接复制行为，也包括摘抄、临摹、录音、录像、拍照、截屏等行为；通过盗窃、贿赂、欺诈、胁迫、电子侵入或者其他不正当手段获取保密信息的行为；
(8) 教唆、引诱、帮助任何主体实施上述行为；
(9) 明知或应知他人违反上述规范，仍然获取、披露、使用、允许他人使用保密信息。
2.4 如果发现乙方保密信息被泄露或者过失泄露保密信息，甲方应当立即采取有效措施防止泄密进一步扩大，并及时向乙方报告。
2.5 如到其他单位任职时，甲方应将自己根据本协议所负有的保密义务如实告知对方。
2.6 甲方承诺，其在本条项下的义务应为持续有效的，不因本协议的终止而终止，也不因其在乙方的工作或服务关系发生终止而终止。甲方离职之后仍对其在乙方任职期间接触、知悉的属于乙方或者虽属于第三方但乙方承诺有保密义务的技术秘密和其他商业秘密信息，承担如同任职期间一样的保密义务和不擅自使用有关秘密信息的义务，而无论甲方因何种原因离职。

第三条 保密期限

3.1 双方同意，甲方离职之后仍对其在乙方任职期间接触、知悉的属于乙方或者虽属于第三方但乙方承诺有保密义务的技术秘密和其他商业秘密信息，承担如同任职期间一样的保密义务，无论甲方因何种原因离职。
3.2 甲方离职后承担保密义务的期限为下列第【 】种（没有做出选择的，视为无限期保密）：
（A）无限期保密，直至乙方宣布解密或者秘密信息实际上已经公开；
（B）有限期保密，保密期限自离职之日起，计算到_____。

第四条 材料、设备及技术资料等的返还

4.1 甲方因职务上的需要所持有或保管的一切记录着乙方秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、磁盘、仪器以及其他任何形式的载体，均归乙方所有，而无论这些秘密信息有无商业上的价值。若记录着秘密信息的载体是由甲方

自备的，则视为甲方已同意将这些载体物的所有权转让给乙方。乙方应当在甲方返还这些载体时，给予甲方相当于载体本身价值的经济补偿。

4.2 经乙方要求，甲方应立即向乙方或其关联公司或合作方（视实际情况而定）归还（并不得继续占有、复制或向他人交付）任何及所有属于乙方或其关联公司或合作方的计算机、盘片、CD、软件、文件、纸张、书籍、资料、档案、收据、车辆、信用卡、信件、手册、记录、其他所有的财产和文件、以及甲方占有和/或控制的任何和全部上述物件的复制件。

4.3 甲方同意，如甲方在其个人财产（如个人电脑）中存有任何乙方保密信息，甲方应向乙方提供该等乙方保密信息的复制件，并将该等乙方保密信息从甲方的个人财产中永久删除。如本款提及的复制或删除因任何原因而无法实现，应乙方要求，甲方应向乙方转移该个人财产的所有权。

4.4 如上述材料属于合作方的，甲方应根据乙方与合作方的约定进行相应材料、设备及技术资料的返还。

第五条 甲方承诺与保证

5.1 甲方承诺，在为乙方履行职务时，不得擅自使用任何属于他人的其他商业秘密，亦不得擅自实施可能侵犯他人知识产权的行为。

若甲方违反上述承诺而导致乙方遭受第三方的侵权指控时，甲方应当承担乙方为应诉而支付的一切费用；乙方因此而承担侵权赔偿责任的，有权向甲方追偿。上述应诉费用和侵权赔偿可以从甲方的工资报酬中扣除。

5.2 甲方承诺，其在乙方任职期间，非经乙方事先同意，不再与乙方生产、经营同类产品或提供同类服务的其他企业、事业单位、社会团体内担任任何职务，包括但不限于股东、合伙人、董事、监事、经理、代理人、顾问等等。

第六条 违约责任

6.1 若一方违反本协议，或未能履行其在本协议项下的任何义务，在中国法律允许的范围内，守约方有权请求强制履行、以及寻求其他任何适当的救济（包括金钱赔偿，如适用）。

6.2 甲方如违反本协议中任何义务，应当承担如下违约责任：

(1) 一次性向乙方支付相当于甲方违约前或离职前（以二者中较早者为准）[十（10）个月]实际所得工资（包括各项奖金）的违约金。甲方的违约行为给乙方造成之损失超过此限的，乙方有权要求甲方另行赔偿（包括但不限于乙方为执行本条款所承担的各项合理费用，如诉讼费、律师费等）。甲方根据本条规定向乙方支付违约金或赔偿乙方损失的，仍应承担本协议项下的相关义务；

(2) 对本协议的违反将被视为严重违反乙方的规章制度，无论违约金给付与否，乙方均有权不经预告立即解除与甲方的聘用关系；

(3) 因甲方的违约行为造成乙方保密信息公开的，甲方应当赔偿该乙方保密信息的全部价值。乙方保密信息的全部价值，可由国家认可的无形资产评估机构评定；

(4) 如甲方因违反本协议下相关义务而获利的，乙方有权要求按照该等获利金额的比例（具体比例届时待乙方确定）作为违约金，要求甲方向乙方支付相应金额。

第七条 争议解决

7.1 因本合同而引起的纠纷，如果协商解决不成，任何一方均有权在乙方所在人民法院提起诉讼。

上述约定不影响乙方通过行政、刑事报案等维权方式提起法律行动。

第八条 其他

8.1 本协议若有未尽事宜，双方可随时协商签订书面的补充协议，补充协议与本协议具有同等法律效力，本合同的修改，必须采用双方同意的书面形式。

8.2 本协议视为乙方与甲方之间劳动合同的附件；本协议与劳动合同、公司章程、规章、管理规约等其他规范文件的相关规定不一致的，应当适用保密义务更高、保密期限更长、保密信息范围更宽的规定或约定。

8.3 本协议任何条款被认定无效、非法或不可执行不影响本协议其他条款的有效性、合法性及可执行性。

8.4 本协议一式两份，双方各执一份，具有同等的法律效力。

8.5 双方确认，已经仔细审阅过本协议的内容，并完全了解本协议各条款的法律含义。

[以下无正文]

甲方（签字）： 乙方（盖章）：

签订日期： 年 月 日 签订日期： 年 月 日

4.3 商务合作保密协议

（甲方和乙方在下文中单独称为“一方”，合称为“双方”）

鉴于：

1. 甲方在经营、研发过程中形成了大量具有重要商业价值的保密信息，且甲方一直采取必要的保密措施，以保护该等信息并防止任何人对该等信息作出任何未经授权的披露或擅自使用；
2. 甲、乙双方形成了业务合作关系，乙方能够获取并知悉甲方的保密信息。

因此，为加强对企业商业秘密的保护，维护双方经济交往中的合法权益，明确乙方的保密义务及责任，依据国家有关法律法规，双方经协商一致，达成如下保密条款：

第一条 保密信息的范围

本协议项下所称“保密信息”指：不为公众所知悉，能为甲方带来经济利益、竞争优势的技术信息和经营信息。该保密信息既包括甲方及其关联公司所有或持有的保密信息，也包括虽属于第三方所有或持有，但甲方负有保密义务的保密信息。保密信息具体包括但不限于：

1.1 技术信息包括但不限于：工作进度、技术方案、工程设计、制造方法、配方、工艺流程、技术指标、研究开发记录、技术报告、测试报告、检测报告、实验数据、试验结果、图纸、样品、模具、操作手册、技术文档、相关的函电等；

1.2 经营信息包括但不限于：双方的合作情况、签署的任何文件，包括合同、协议、订单等文件中所包含的一切信息、客户名单、行销计划、采购资料、定价政策、财务资料、进货渠道、供应产品信息、供应商评审要求及价格、法律事务信息、人力资源信息等；

1.3 其他根据行业惯例、公司规定、双方约定应当保密的重要资料。

第二条 保密责任和义务

2.1 乙方承诺对甲方上述保密信息，以及所接触到的与甲方及其关联公司有关的其他机密资讯或文件资料保密，遵守甲方的保密制度，执行有关的保密程序。

2.2 乙方应采取所有必要的合理措施保护甲方的保密信息免遭未经甲方许可的披露或使用，包括执行有效的安全措施和操作规程。

2.3 乙方不得通过任何途径将甲方保密信息向任何第三方进行披露或泄漏。乙方不得以与甲方正常业务合作之外的目的私自使用甲方保密信息，或者允许外部人员或内部非本职工作人员使用甲方保密信息，并有义务采取措施确保相关责任方内部相互监督，实行保密义务。否则，给甲方造成损失的，由乙方与相关责任方承担连带责任。

2.4 双方合作终止时，乙方应于十（10）天之内将所接收的所有甲方保密信息（包括但不限于以任何形式存在的保密信息的原件、复印件、复制品和对保密信息的概述摘要）完全移交给甲方或甲方指定人员，不得以任何形式私自占有及带出甲方公司。

2.5 如乙方发现保密信息泄露或资料遗失，或上述事由有发生之虞时，乙方应立即通知甲方，自行采取适当措施或配合甲方采取措施弥补因保密信息泄露或资料遗失所造成的损失。

2.6 乙方应尽力配合甲方的人员管理和正常的业务流程，不主动与相关业务员进行私下联系，给予或许诺给予贿赂或好处，以寻求不正当的商业利益。对此，如果造成甲方损失的，甲方有权以违约或侵权行为向乙方要求赔偿，直至追究相关责任人的刑事责任。

第三条 保密期限

乙方应承担保密义务的期限为无限期保密，直到甲方公开披露或保密信息实际上已经公开。

第四条 违约责任

乙方如违反本协议中所涉任何条款，应赔偿甲方因此所受到的一切直接及间接损失。本协议所称损失应包括因乙方违约行为所导致的甲方相关损失，以及甲方为处理违约行为所发生的包括律师费、调查取证费、差旅费、诉讼费以及其他相关费用和开支。

第五条 争议的解决

5.1 本协议的成立、生效、履行、解释、执行及争议解决等相关事宜均适用中华人民共和国法律。

5.2 因本协议引起的或与本协议有关的任何争议，双方应友好协商解决；若协商不成的，任何一方有权将争议提交至甲方住所地有管辖权的人民法院诉讼解决。

第六条 双方确认

双方确认，在签署本协议前已仔细审阅过协议的内容，并完全了解协议各条款的法律含义。

第七条 协议的效力

7.1 本协议自双方签署之日起成立并生效。

7.2 本协议经双方书面同意，可以予以修改、补充或调整。就本协议未尽事宜，双方可另行签订补充协议，补充协议为本协议有效组成部分。

7.3 本协议一式二份，甲、乙双方各执一份，均具同等效力。

[以下无正文]

甲方（盖章）：　　乙方（盖章）：

签订日期：　　年　月　日　　签订日期：　　年　月　日

上海市市场监督管理局执法总队

金杜律师事务所
KING&WOOD
MALLESONS

北京市金杜律师事务所

Linemore 蓝盟

上海蓝盟网络技术有限公司