ICS 03.100.01
CCS A 01

T/NBQLX

宁波市汽车零部件产业协会团体标准

T/NBQLX 003-2025

汽车零部件企业商业秘密保护规范

Specification for trade secret protection of auto-parts enterprises

2025－07－30 发布　　2025－08－01 实施

宁波市汽车零部件产业协会　　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。

本文件由宁波市市场监督管理局提出。

本文件由宁波市汽车零部件产业协会归口。

本文件起草单位：宁波市汽车零部件产业协会、宁波市海曙区市场监督管理局、宁波市标准化研究院、宁波帅特龙汽车系统股份有限公司、宁波圣龙汽车动力系统股份有限公司、宁波均胜群英汽车系统股份有限公司、中汽研汽车检验中心（宁波）有限公司、宁波旭升集团股份有限公司、富诚汽车零部件有限公司、宁波申江科技股份有限公司、宁波继峰汽车零部件股份有限公司、山子高科技股份有限公司、宁波思明汽车科技股份有限公司、宁波信跃电子科技有限公司、宁波巨航冷挤科技有限公司、宁波市四通达模具科技有限公司、宁波中桓联合科技咨询有限公司、宁波市雷龙凯力达技术有限公司、宁波科诺精工科技有限公司。

本文件主要起草人：汪虹、马斌、陈可梁、于海滨、伍晓茜、周山山、邬米娜、姚立、余美珍、朱晓勇、洪露、贺娜、唐铭杰、张伟明、吴荣生、李勤华、章玉明、吕方、沈银川、徐昊、毛志方、丁超、应杰侠、张龙、张娜。

汽车零部件企业商业秘密保护规范

1 范围

本文件规定了汽车零部件企业商业秘密保护的术语和定义、基本要求、商业秘密范围、组织机构、涉密事项管理、维权管理、应急管理、评估与改进等内容。

本文件适用于汽车零部件企业的技术信息和经营信息等商业秘密的保护管理。

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。

DB33/T 2273-2020 商业秘密保护管理与服务规范

3 术语和定义

DB33/T 2273-2020界定的以及下列术语和定义适用于本文件。

3.1

涉密人员 secret personnel

根据工作职责或者保密协议有权接触、使用、掌握商业秘密的企业员工、供应商、客户或其他人。

3.2

涉密设备 secret device

生成、存储、处理商业秘密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。

3.3

涉密区域 secret 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、研发室、实验室、办公室、保密室、档案室、机房、用户现场等。

4 基本要求

4.1 企业商业秘密保护管理应遵循“依法规范、企业自主、预防为主和全面覆盖”的原则。

4.2 应全面统筹商业秘密保护的目的、载体、路径等，将商业秘密与专利、商标、著作权等系统布局，立体保护。

4.3 应加强商业秘密前置保护，可自建或使用符合国家标准、行业标准的商业秘密存证平台，实施预先存证保护措施。

5 商业秘密范围

5.1 企业应根据自身情况界定商业秘密的范围，商业秘密一般分为技术信息和经营信息。

5.2 技术信息是指与技术有关的结构、原料、组分、配方、材料、样品、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。包括但不限于：

a) 设计图纸，如汽车底盘零部件图纸、电池模组设计图、电机结构图、模具工装设计资料等；
b) 材料信息，如使用的特殊合金、复合材料、涂层配方、热处理工艺参数等；
c) 工艺参数，如精密制造工艺、材料配方、模具加工参数、设备成型加工参数等；
d) 研发数据，如电池能量密度测试数据、电机效率优化实验记录、产品及工艺仿真分析数据等；
e) 技术方案，如未申请专利的创新技术、生产工艺流程技术等；
f) 智能化零部件技术细节，如智能驾驶系统的控制算法和车路协同技术的核心代码等软件算法；域控制器架构、传感器集成方案等硬件设计等；
g) 数据资产与数字技术，如生产能耗数据、设备运维日志等工业互联网数据以及区块链存证信息等；
h) 性能测试数据与报告，如原型在台架测试、道路测试、环境测试、耐久性测试、碰撞测试等过程中产生的原始数据、分析结果、性能参数、失效模式分析报告；
i) 仿真数据，如零部件系统结构强度、流体动力学、热管理性能等的仿真分析数据等；
j) 市场反馈数据：零部件售后故障统计分析、竞品技术对标分析报告、市场需求调研分析结论等；
k) 计算机程序，如软件源代码、系统作业指导书、网络拓扑图等；
l) AI 与大数据技术，如自动驾驶训练数据集、AI 模型参数等；
m) 绿色技术，如新能源汽车电池回收工艺、碳足迹数据等；
n) 供应链技术，如零部件全球供应链实时监控系统算法等。

5.3 经营信息是指与经营有关的创意、管理、销售、财务、计划、样本、招投标材料、客户、数据等信息。包括但不限于：

a) 客户资料，如客户信息（客户的名称、地址、联系方式以及交易习惯、意向、内容等信息）、长期合作的整车厂客户信息、订单需求预测数据等；
b) 供应商信息，如关键原材料采购渠道、价格协议、合作条款等；
c) 市场策略与商业计划，如成本核算模型、价格浮动机制、未公开的新产品（车辆、部件、零件）的影像资料、市场推广计划；
d) 生产与质量控制信息，如质量管理体系、自动化产线布局、设备及工艺参数设置等；
e) 国际合作与跨境数据，如海外工厂布局、技术授权协议条款、通过加密网关传输的客户订单数据等。
f) 产品询价与定点信息，如新产品报价信息，产品包装设计方案，产品成本分解资料，产品生产工艺设计流程等；
g) 财务数据，如未公开的财报、税务方案、银行授信额度等；
h) 影响环境、社会和公司治理的相关数据，如未公开的环保合规报告、社会责任审计结果等。

6 组织机构

6.1 应构建领导责任、监管责任、主体责任于一体的商业秘密保护管理体系。

6.2 决策层应具备商业秘密保护意识，并履行商业秘密保护的领导责任；

6.3 应设立商业秘密保护部门/机构，职责主要包括：

——组织制定商业秘密保护制度，监督、检查制度落实情况，并定期进行评估和改进；
——识别和管理商业秘密事项，如涉密的部门、人员、物品、区域；

——执行领导机构的决策决议；
——制定并动态更新商业秘密事项清单；
——组织商业秘密保护培训；
——指导、监督业务部门制定、实施商业秘密保护方案；
——组织内部商业秘密风险隐患排查与整治；
——处理泄密或侵犯商业秘密事件。

6.4 业务部门应由部门负责人为部门商业秘密管理责任人，负责各自范围内企业的生产、经营等商业秘密的保护。重点业务部门宜配备专职保密员。

7 涉密事项管理

7.1 应对确定的商业秘密进行分类分级，按照密级高低实行分级保护和管理。商业秘密宜分为核心秘密、重要秘密、一般秘密。

——核心秘密：泄露会使企业权益和利益遭到特别严重损害的信息。
——重要秘密：泄露会使企业权益和利益遭受严重损害的信息。
——一般秘密：泄露会使企业权益和利益遭受损害的信息。

7.2 应制定商业秘密保护清单，并对商业秘密进行标识。

7.3 应明确商业秘密的保护事项，并建立对涉密人员、涉密载体、涉密物品、涉密区域、涉密商务活动等事项的管理要求，采取相应的保护措施。

7.4 商业秘密保护的具体管理内容和措施参见附录 A。

8 维权管理

8.1 证据收集

8.1.1 应及时收集并固定以下证据材料，必要时可进行证据保全公证。

a) 商业秘密权属证明，主要包括：
——研发立项、记录文件、试验数据、技术成果验收备案文件等证明材料；
——商业秘密交易转让合同或授权使用许可协议等证明材料。
b) 商业秘密的具体内容和载体；
c) 商业秘密不为公众所知悉的证明，主要包括：
——在汽车零部件产业不属于一般常识或者行业惯例；
——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不能通过观察上市产品即可直接获得；
——未在公开出版物或者其他媒体上公开披露；
——未通过公开的报告会、展览会等方式公开；
——所属领域的相关人员无法从其他公开渠道获得。
d) 商业秘密具有商业价值的证明，主要包括：
——生产经营活动中形成的阶段性成果；
——研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的持续时间。
e) 已对商业秘密采取相应保护措施的证明，主要包括：
——签订保密协议或者在合同中约定保密义务；
——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；

——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；
——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；
——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；
——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。

f） 可能与泄密信息有关的人员信息，主要包括：
——有关人员在本单位的工作经历、工作内容、接触到的涉密信息以及其他有可能、有条件接触到商业秘密的证明材料；
——有关人员在本单位接受保密培训的记录；
——有关人员与本单位签订的保密协议。

g） 侵权信息与企业商业秘密相同或者实质相同的证明材料；
h） 侵犯商业秘密的具体行为表现；
i） 侵犯商业秘密行为导致的后果。

8.1.2 商业秘密的非公知性、同一性等专业技术事项可委托第三方机构进行鉴定。

8.2 维权途径

8.2.1 根据证据收集情况，企业可依法采取下列维权方式：
——和解与调解；
——寻求行政保护；
——申请商事仲裁；
——寻求司法保护。

8.2.2 和解与调解的维权方式主要包括以下内容：
——通过协商和解方式解决商业秘密侵权纠纷，在和解协议中约定赔偿金额、保密义务等条款；
——可以基于实际的商业谈判情况和具体的商业需求，在符合法律现定的情况下，约定竞业禁止等条款；
——与侵权人双方委托共同认可的政府机构或社会机构进行调解，或由人民法院委派调解机构进行诉前、诉中调解。

8.2.3 寻求行政保护的维权方式主要包括以下内容：
——向违法行为发生地的县级以上市场监督管理部门举报，并按要求提供材料；
——根据案件进展情况，在立案后变更、增加其所主张的商业秘密具体内容；
——经核查立案后，应配合市场监督管理部门的调查取证工作。

8.2.4 商事仲裁的维权方式指违反协议约定的保密义务并且约定商事仲裁管辖条款的,若尚未构成刑事犯罪的,企业可向约定的仲裁委员会申请仲裁。

8.2.5 涉及国家秘密的，应立即采取补救措施，并向当地公安机关、国家安全机关和保密行政管理部门报告。

8.2.6 司法保护方式指权利人对于商业秘密收到他人侵犯的，可以向人民法院提起民事诉讼；如果构成犯罪的，可以向公安机关进行控告。

9 应急管理

9.1 应制定商业秘密泄密或侵权的应急处理预案，内容主要包括：

——应急小组成员及其职责；
——紧急应对流程；
——泄密或侵权溯源和评估定级方案；
——防止信息进一步扩散、危害和损失扩大的应急措施方案；
——维权方案；
——总结和改进方案。

9.2 紧急应对流程主要包括事件上报、成立应急小组、核查确认泄密或侵权内容、评估泄密或侵权事件等级、应急处置、维权和责任追究、形成事件报告、提出整改方案等。

9.3 可从以下几方面对泄密或侵权事件进行评估定级：
——涉及的商业秘密等级和数量；
——侵权的方式，如未经许可的复制、向第三方披露、被公开、被第三方使用；
——事件对企业造成的影响；
——泄密或侵权嫌疑人的情况；
——其他影响泄密或侵权事件评估分级的因素。

9.4 出现商业秘密泄露的迹象时，企业可采取以下措施防止信息扩散：
——涉密载体、物品等失窃或被未经许可复制的，应保护现场并调查、确定泄密范围和流向，及时追回被窃涉密载体、物品或复制后的版本；
——明确泄密后 4 小时内启动证据固定、法律保全等动作；
——商业秘密被上传至信息系统、互联网或其他未被允许渠道公开的，应联系相应渠道的运营方或信息管理部门对泄露信息进行屏蔽或删除；
——向侵权嫌疑人发送侵权告知函；
——向法院申请保全措施；
——与专业机构合作处理舆情，如技术泄露被公开报道时的舆情处理。

9.5 应加强对员工的相关培训和引导。

9.6 应定期开展应急演练，做好演练信息的记录和存档。

10 评估与改进

10.1 评估

10.1.1 企业应对商业秘密保护管理情况进行监督检查，确保其持续的适宜性、充分性和有效性。

10.1.2 应制定监督检查方案，内容主要包括检查的内容、方法、频次，检查人员的职责和权限，检查结果的运用和整改等。

10.1.3 监督检查内容应主要包括：
——商业秘密的定密、分级、流转；
——涉密人员、载体、物品、区域等的管理情况；
——涉密商务活动管理情况；
——操作系统、办公软件、信息系统等工具软件的账号、权限、密码管理和使用商业秘密情况；
——商业秘密保护管理制度建立和实施情况。

10.1.4 监督检查方法应主要包括：
——调取涉密载体、涉密物品、涉密信息使用记录、涉密区域出入口和内部监控、操作系统、办公软件、信息系统等工具软件的日志文件、涉密活动记录及附属合同等相关工作材料；
——现场查验、问询涉密人员。

10.1.5 应根据监督检查结果形成评估报告。

10.1.6　可委托第三方机构开展评估。

10.1.7　业务流程变更、系统软件导入/变更需评估对商业秘密保护的风险，影响程度。

10.1.8　定期识别评审商业秘密的范围，并从人员资源、硬件/环境、软件/系统、服务/其他等方面识别支持性资产可能导致商业秘密泄露的风险以及风险处置方法。

10.2　改进

10.2.1　应对监督检查发现的问题制定整改计划，并持续改进。

10.2.2　应对改进情况进行复查、复评。

10.2.3　应对评估中发现的问题及时改进。

10.2.4　应鼓励企业员工提供保密建议，建立举报机制，对举报人进行奖励。

附 录 A
（资料性）
商业秘密保护管理具体内容

A.1 定密、脱敏处理、解密和消密

A.1.1 定密

A.1.1.1 应对商业秘密进行核查和评估，其表现形式、评估范围主要包括：

——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；

——其他的具有价值的商业信息。

A.1.1.2 应拟订商业秘密保护项目文件，内容包括商业秘密的类别及名称（代码）、保密期限、知悉范围、涉密人员范围、价值估算、保护措施及泄露损失等。

A.1.1.3 应定期对商业秘密保护项目的密级进行复评。当出现以下情形之一的，应即刻变更密级：

——法律法规或政策调整，使项目密级出现变化；

——因工作需要或人员变动，项目知悉范围发生较大变化；

——保密期限发生变化；

——商业秘密泄露后对企业带来的影响发生变化。

A.1.2 脱敏处理

A.1.2.1 下列情形涉及商业秘密的，应对信息进行隐藏：

——与供应商、客户、合作方等的沟通和信息往来中；

——信息公开、发布、流转时；

——协助其他单位尽职调查时；

——其他情形。

A.1.2.2 脱敏处理的方式包括隐藏、删除或模糊化处理等。

A.1.2.3 在配合行政机关和有关部门进行行政检查或执法行动时，应主动提醒执法检查人员对商业秘密履行保密义务。

A.1.3 解密

A.1.3.1 应根据商业秘密级别自行设定保密期限：

——可以预见时限的，以年、月、日计；

——不可预见时限的，可定为“长期”或“公布前”。

A.1.3.2 解密应满足以下要求：

——保密期限已满，经商业秘密保护部门/机构评估后确定已不再具有保护价值的；

——企业认为商业秘密事项已不再具有保护价值的；

——其他特定因素导致商业秘密被公开的。

A.1.3.3 解密方式包括消除密级标识与提示、移出涉密区域、电子文档解密等。

A.1.4 销密

A.1.4.1 保密员制定需销毁的涉密实物、载体及电子文件清单，提交商业秘密保护部门/机构评估与审批确认。

A.1.4.2 销毁方式主要包括：

——文件、资料应粉碎成颗粒状或焚烧处置；

——电子信息应利用彻底删除软件永久删除；

——含有核心秘密的电子信息载体应作销毁处理。

A.1.4.3 应对销毁过程实施监督，方式主要包括：

——视频监控；

——不少于 2 名员工见证下销毁；

——对销毁过程录像等。

A.2 涉密人员管理

A.2.1 基本要求

A.2.1.1 应按涉密程度，将涉密人员分为核心涉密人员、重要涉密人员和一般涉密人员，并分类管理。

A.2.1.2 挂职、实习等人员应参照涉密人员管理。

A.2.2 入职管理

A.2.2.1 应对涉密岗位的拟入职人员进行背景调查，主要包括刑事记录核查和社交媒体风险筛查等。并核实其与原单位签署的保密协议，要求其不应泄露前雇主商业秘密。

A.2.2.2 应与新入职涉密人员（含转岗）签订与其岗位工作相适应的保护协议，并签订竞业限制协议。

A.2.2.3 宜与高级管理人员、高级技术人员及其他负有保密义务的人员（如研发、财务、采购、销售等涉密重点岗位人员）签订竞业限制协议。

A.2.2.4 应定期对在职员工进行业务内容审核，以排除其使用原单位商业秘密。

A.2.3 培训管理

A.2.3.1 应建立涉密预防培训管理制度，并制定年度培训管理计划。培训内容主要包括：涉密应遵守的规则，涉密会涉及商业秘密的说明，涉密观看及留置、路径管理要求，涉密停留区说明等内容。

A.2.3.2 应每年对涉密员工进行商业秘密保护培训，可采取发放资料、集中培训、网络培训或相结合的方式开展培训。

A.2.3.3 应对新入职涉密岗位的人员进行商业秘密保护培训。

A.2.3.4 签订员工保密合同/协议的人员在培训结束后宜进行考核。

A.2.3.5 应做好培训及相关考核记录，并保存。

A.2.4 履职管理

A.2.4.1 应经商业秘密保护部门/机构审批后方可开展以下行为：

——登陆未授权账户或系统；

——超范围使用涉密文件资料、物品、数据；

——复制、发送涉密电子文档；

——将涉密电子文档存于未授权载体或网终空间；
——拍摄、摘抄涉密资料；
——进入非授权涉密区域；
——披露企业未公开的信息。

A.2.4.2 应督促员工做好本岗位商业秘密保护工作：
——涉密信息及载体应及时上报，由保密员归档统一管理；
——使用涉密信息应履行登记手续；
——涉密电子文档、数据按规定途径和要求使用、流转等；
——离开工作岗位前及时下线工作账户，或设置电脑锁屏等。

A.2.4.3 定期进行商业秘密保护教育培训，并保存培训记录。

A.2.5 离职管理

A.2.5.1 对涉密岗位员工转岗、离职的脱密措施主要包括：
a) 清退员工以下涉密载体和物品，由部门负责人复核确认：
——涉密文件、数据及其载体、物品；
——办公账号、密码等账户信息；
——工作电脑；
——门禁卡、钥匙等。
b) 组织离职谈话，告知其不应有以涉密下行为：
——复制、带离、损毁、篡改、拍摄涉密文件资料、物品；
——查阅、拷贝、篡改、发送涉密电子文档、数据；
——删除、更改账户；
——披露、使用商业秘密。
c) 开展离职检查并做好书面记录，检查内容包括:
——工作电脑数据是否完整；
——工作账户是否有异常操作，如异常查询、下载、拷贝、修改、删除等；
——是否有对外发送商业秘密信息的记录；
——是否有权限之外的文档、信息数据等；
——离职前一定期限内的涉密信息查阅和使用情况等。
d) 与其签订离职离岗保密承诺书。

A.2.5.2 应及时通知与转岗、离职员工有关的供应商、客户、合作单位等，做好业务交接。

A.2.5.3 及时掌握离职员工在竞业限制期限内的任职去向。

A.2.5.4 因特殊原因被公司辞退人员，需第一时间禁用其账号（主要包括 AD\邮件等），并回收其电脑，避免造成资料泄露的隐患。

A.3 涉密载体管理

A.3.1 一般要求

A.3.1.1 应由商业秘密保护部门/机构统一登记、保存，未经审批不应转移、拍摄、仿造、测绘、破坏。

A.3.1.2 应采用物理隔离方式存放在涉密区域。

A.3.1.3 转移维修前应经商业秘密保护部门/机构审批，并拆卸涉密存储设备。

A.3.2 电子载体管理

对电子载体的管理措施主要包括：

——涉密非移动电子载体宜禁用移动存储、光驱、蓝牙等数据传输功能，未经权限审批不得随意安装软件；

——涉密移动电子载体宜设置身份识别等加密措施，不可接入非涉密或未采取保密措施的电子设备；

——对涉密电子载体的制作、使用、保存、维修、销毁实施全生命周期管理，履行审批和登记手续，由专人负责并建立台账；

——涉密电子载体不应擅自外送维修，外送维修前宜经商业秘密保护部门/机构审批，并拆卸涉密存储设备或解除涉密信息。

A.3.3 纸质文档管理

对涉密纸质文档的管理措施主要包括：

——有密级、保护期限等标识的，实行登记管理归档存放；

——存放在涉密区域内并由专人管理；

——按权限使用，履行审批和登记手续；

——废弃涉密纸质文档宜由专人进行销毁。

A.3.4 信息系统管理

对涉密信息系统的管理措施主要包括：

——合理设定不同账户的权限，主要包括：

a) 不同层级账户的功能和审批权限；

b) 项目中不同账户的功能和使用期限；

c) 不同账户的访问、操作、查看权限和使用期限以及互联网使用权限。

——对涉密信息系统采取密码管理的方式：

a) 不使用默认密码，不可设置保存密码自动登录功能；

b) 限制设置简单密码；

c) 不定期更改密码，最长间隔时间不宜超过三个月；

d) 输错密码一定次数锁定账户；

e) 同一用户登录不同涉密信息系统宜采用不同密码，确保密码唯一性；

f) 设置生物识别进行密码双重验证。

——宜对所有涉密账号和密码实行统一登记、备案、发放和变更管理；

——权限到期、人员转岗、项目或事项变更时及时回收、变更系统权限；

——在涉密信息系统内设置保密义务提醒；

——做好病毒防范、查杀和病毒库的升级等工作；

——定期进行安全检查，发现系统漏洞及时修补；

——定期对涉密信息系统的数据、日志等进行备份并妥善保管；

——信息系统的管理员权限宜在不同员工之间进行分配。

A.3.5 电子数据管理

对涉密电子数据的管理措施主要包括：

——应存储在企业授权的存储设备和应用系统或云存储空间；

——核心秘密、重要秘密等级的数据应采用加密方式存储，并定期备份后妥善保存；

——解密应由专人操作，员工按权限使用加密数据；

——收发涉密数据宜使用唯一出入口，并对过程进行审批；
——内部局域网宜与互联网隔离，涉密数据网络传递宜通过内部局域网或加密互联网通道完成；
——通过邮件发送涉密数据时，宜加密和签名，可限定打开次数、打开时限和编辑权限；
——对外发送涉密数据应经过审批，并采取加密措施，数据发送与密钥发送不宜采用同一通道；
——宜对涉密数据拷贝采取限制措施，拷贝宜履行审批手续并妥善保存拷贝记录；
——涉密电子数据宜做好公证、第三方存证、电子存证等证据固定；
——涉密电子数据销毁时宜确保彻底永久删除。

A.3.6 区域管理

A.3.6.1 应设置涉密区域的地点或部门主要包括：
——研发设计、信息管理、财务、人力资源部门核心区域；
——实验室、重要生产工作场所；
——控制中心、服务器机房等；
——涉密档案、涉密载体存放地点；
——未公开的样品存放地点；
——模具、专用夹具、重要零部件等的存放区；
——重要原材料、重要半成品等涉密物资存放区等。

A.3.6.2 对涉密区域的管理措施主要包括：
——宜设置物理隔离，形成独立、封闭的区域并设置门禁，张贴明显标识和警示语；
——出入口安装监控设施和报警装置，采用有效技术手段对出入人员进行身份验证；
——出入涉密区域人员应履行权限审批和登记手续；
——来访人员访问应经审批，进出登记并佩戴访问证件；
——宜限制使用具有录音、拍照、摄像、信息存储等功能的电子设备；
——必要时采取网络隔离阻断。

A.4 涉密活动管理

A.4.1 商务活动

A.4.1.1 在商务活动中涉及商业秘密的，应对相关信息进行隐藏，包括隐藏或删除涉密信息、对涉密信息进行模糊化处理等方式。

A.4.1.2 对商务合作活动的管理措施主要包括：
——开展商务合作、共同开发、委托加工等商务活动时，签订保密协议约定保密义务；
——聘任可能接触涉密信息或涉密物品的外部人员时，签订保密协议，必要时可做背景调查；
——对合作过程进行控制，对涉密信息或物品的使用情况进行监督管理。

A.4.2 访问、参观、检查

对访问、参观、检查等活动的管理措施主要包括：
——来访人员应履行审批和登记手续；
——安排专人陪同访问、参观，限制拍照、录音、录像、信息存储等行为；
——政府部门因检查、监督等工作需要接触涉密信息或涉密物品的，提前向其明示保密义务。

A.4.3 涉密会议或其他活动

A.4.3.1 涉及商业秘密的会议或其他活动的管理措施主要包括：

——选择具有保密条件的场所；
——限定参加人员的范围，指定参与涉密事项的人员；
——告知参加人员保密要求，必要时签订保密承诺书；
——对涉密文件、资料控制发放范围，做好发放登记，及时收回清点；
——通过拍照、摄像、签名等方式，做好记录等。

A.4.3.2　涉及商业秘密的远程工作，宜采取下列保密措施：

——经商业秘密保护部门/机构审批；
——对远程网络进行安全鉴别；
——规定硬件和软件的支持与维护要求；
——规定远程工作的环境安全要求；
——授权访问人员，设置访问权限；
——配备专用的操作和存储设备，防止使用私有设备处理或存储信息；
——进行安全监视和过程审核，形成记录；
——远程工作终止时，撤销授权和访问权限；
——其他有必要的保护措施。

参 考 文 献

[1] 《中华人民共和国民法典》
[2] 《中华人民共和国反不正当竞争法》
[3] 《中华人民共和国劳动合同法》
[4] GB/T 22080《网络安全技术 信息安全管理体系 要求》