ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T XXXXX—XXXX

工业数据要素型企业建设指南

Guidelines for construction of industrial data element-oriented enterprises

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　　言 IV
引　　言 V
1 范围 6
2 规范性引用文件 6
3 术语和定义 6
4 总体原则 7
5 总体框架 8
6 数据战略与组织保障 8
6.1 战略规划 8
6.2 治理组织 8
6.3 职责体系 9
6.4 制度体系 9
6.5 人才体系 9
6.6 文化与变革管理 9
7 工业数据资源与治理体系 9
7.1 数据范围 9
7.2 资源盘点 9
7.3 数据目录 9
7.4 数据采集与汇聚 10
7.5 外部数据管理 10
7.6 数据架构与模型 10
7.7 数据标准 10
7.8 主数据与参考数据 10
7.9 数据质量 10
7.10 元数据与血缘 11
7.11 指标与标签 11
7.12 工业高质量数据集 11
7.13 工业知识 11
7.14 数据生命周期 11
8 数据基础设施与技术体系 11
8.1 技术架构 11
8.2 边缘采集与连接 12
8.3 数据集成与处理 12
8.4 存储与计算 12
8.5 开发治理工具 12
8.6 数据服务 13

8.7 工业模型 13
8.8 流通利用基础设施 13
8.9 运行维护与连续性 13
9 工业数据要素场景应用 14
9.1 体系设计 14
9.2 应用识别 14
9.3 方案设计 14
9.4 应用建设 14
9.5 应用推广 14
9.6 价值度量 14
10 数据价值化与流通机制 15
10.1 总体要求 15
10.2 内部共享 15
10.3 跨主体流通 15
10.4 权益与授权管理 15
10.5 数据产品与服务 15
10.6 价值评价 16
10.7 成本核算与收益分配 16
10.8 数据产品运营监测 16
11 安全合规与风险管理 16
11.1 安全责任 16
11.2 分类分级 16
11.3 合规与权益保护 16
11.4 流通风险评估 17
11.5 权限与使用控制 17
11.6 数据安全防护 17
11.7 模型安全防护 17
11.8 审计溯源与监测 17
11.9 应急处置与恢复 17
11.10 数据跨境 17
11.11 第三方机构安全管理 17
12 数据生态协同 18
12.1 内部协同 18
12.2 产业链供应链协同 18
12.3 外部服务协同 18
12.4 成果推广 18
13 数据要素效能评价与改进 18
13.1 评价机制 18
13.2 评价指标 18
13.3 评价实施 19
13.4 评价结果与改进 19
附录 A 20

参 考 文 献 22

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。

本文件为GB/T 《工业数据要素型企业能力要求》。

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。

本文件全国信息技术标准化技术委员会（SAC/TC28）提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国南方电网有限责任公司、中国第一汽车集团有限公司、海尔智家股份有限公司、国家能源投资集团有限责任公司、煤炭科学研究总院有限公司、新特能源股份有限公司、南方电网数据平台与安全（广东）有限公司、国家数据集团、北京赛西科技发展有限责任公司、北京易华录信息技术股份有限公司、北京三维天地科技股份有限公司、南方电网能源发展研究院有限责任公司、数久科技（北京）有限公司、贵州电网有限责任公司、湖北华中电力科技开发有限责任公司、中国船舶综合技术经济研究院、南方电网人工智能科技有限公司、国网新疆电力有限公司营销服务中心、中科斯欧（合肥）科技股份有限公司、上海零数众合信息科技有限公司、国网江西省电力有限公司、中国石油天然气股份有限公司新疆油田分公司、建筑材料工业信息中心、北京国建信联科技发展有限公司

本标准主要起草人：李成博、李冰、楼瑶、陈彬、杨秋勇、张硕、杨少明、夏玉萍、闫计栋、郑浩、张建中、王浩、丁国原、李西良、曹熙、马一宁、缪新萍、张建荣、倪志云、王兆君、林荣政、郭彦楠、张岩、尚迪雅、陈红、朱昌会、李振军、艾艳可、肖益、许洁、白雪、赵晓晗、孙怡、权环宇、高立伟、宋博宇、朱姝睿、胡之恒、王昊、杨兴源、袁怀玉、林正清、姚晗、黄嘉懿、赵翔宇、冯勤宇、江佳佳、王永超、宣秀芳、郭军、于万钦、兰春嘉、杨珍、王璠、赵金玲、张闻晨、胡雅涵、袁英敏、毕昆

引　言

数据作为新型生产要素，已深度融入工业研发设计、生产制造、经营管理、客户服务和产业协同等环节。推进工业数据从资源化、知识化向要素化、价值化演进，有助于促进生产方式变革、经营效率提升、产业链供应链协同和新模式新业态培育。

工业数据具有来源多样、类型复杂、实时性强、专业关联度高以及商业秘密和重要数据集中等特点。企业建设工业数据要素能力，既要强化数据采集、汇聚、治理、开发和应用，也要建立权责清晰、安全可控、可持续运营的数据流通利用机制。

本文件以需求牵引、场景驱动和价值实现为导向，将安全要求贯穿数据供给、流通和使用全过程，系统提出战略治理、数据资源、技术支撑、场景应用、流通运营、安全合规、生态协同、实施评价等方面的建设指导，为不同规模、不同发展阶段的工业企业提供可裁剪、可实施、可评价的参考。

工业数据要素型企业建设指南

1 范围

本文件给出了工业数据要素型企业建设的总体原则、建设目标与框架，以及战略治理、数据资源与治理、技术支撑、场景应用、流通利用、安全合规、生态协同和评价改进等方面的指导。

本文件适用于工业企业开展数据要素能力的规划、建设、运营和持续改进，也可为工业互联网平台企业、数字化转型服务商、行业组织及有关第三方评估机构提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35295—2017 信息技术 大数据 术语

GB/T 36073—2015 数据管理能力成熟度评估模型

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 43697—2024 数据安全技术 数据分类分级规则

GB/T 39116—2020 智能制造能力成熟度模型

3 术语和定义

下列术语和定义适用于本文件。

1.1

工业数据 industrial data

工业数据是指工业各行业各领域在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

1.2

数据要素 data element

数据要素是指以电子形式存在的、通过计算的方式参与到生产经营活动并发挥重要价值的数据资源。

1.3

工业数据要素型企业 industrial data element-oriented enterprise

将工业数据作为关键生产要素，持续开展数据采集、汇聚、治理、开发、应用和流通利用，通过数据驱动工业研发设计、生产制造、供应链、产品销售、服务等业务环境创新和产业协同，并建立相应组织、技术、运营和安全保障机制的企业。

1.4

工业数据产品 industrial data product

以工业数据为主要加工对象，经治理、分析或模型化处理形成，可满足特定业务需求并能够以数据集、数据接口、数据报告、数据模型、数据应用等形态提供的产品。

1.5

工业数据服务 industrial data service

围绕工业数据的采集、治理、开发、应用、流通、安全和运营等活动，向数据使用方提供的专业化服务。

1.6

高质量工业数据集 industrial high-quality dataset

数据面向特定工业场景，经过采集、加工等数据处理，可直接用于开发和训练人工智能模型，能有效提升模型性能的数据的集合。

1.7

工业知识 industrial knowledge

对工业对象、机理、工艺、规则、经验、案例及其关联关系进行结构化表达，可用于分析、推理、决策或控制的知识资源。

1.8

数据流通利用 data circulation and utilization

数据在不同主体或不同业务单元之间，按照约定目的和规则进行提供、共享、开放、授权使用、加工处理或交易，并产生使用价值的活动。

1.9

可信数据空间 trusted data space

基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。

4 总体原则

工业数据要素型企业建设宜遵循以下原则。

a) 战略统筹：宜将工业数据要素建设纳入企业发展和数字化转型总体规划，统筹业务、数据、技术、安全和生态建设。
b) 需求牵引：宜从真实业务需求和可量化价值出发选择建设任务，以场景应用检验数据治理与平台能力。
c) 统一规范：宜统一数据架构、目录、模型、标准、质量和接口要求，推进源头治理和跨系统一致性管理。
d) 分类施策：宜根据行业特征、企业规模、建设阶段、数据风险和场景需求选择适宜的建设范围、方式和强度。
e) 开放协同：宜在保障合法合规和商业秘密的前提下，促进企业内部、产业链上下游以及相关服务主体之间的数据协同。
f) 安全可控：应将安全贯穿数据供给、流通、使用、归档和销毁全过程，依据数据类别、级别和应用场景实施差异化保护。
g) 价值闭环：宜建立从场景识别、数据供给、应用验证、价值度量到持续改进的闭环，形成可持续运营机制。

5 总体框架

总体框架由价值目标、工业场景、数据价值链、能力底座和保障体系构成。价值目标包括提质、增效、降本、绿色、安全和创新；工业场景覆盖研发设计、生产制造、经营管理、客户服务和产业协同；数据价值链覆盖采集、汇聚、治理、开发、服务、流通、使用和评价。

能力底座包括数据资源、标准规范、平台工具、模型知识和安全合规能力；保障体系包括战略组织、制度机制、人才投入、项目管理和生态协同。

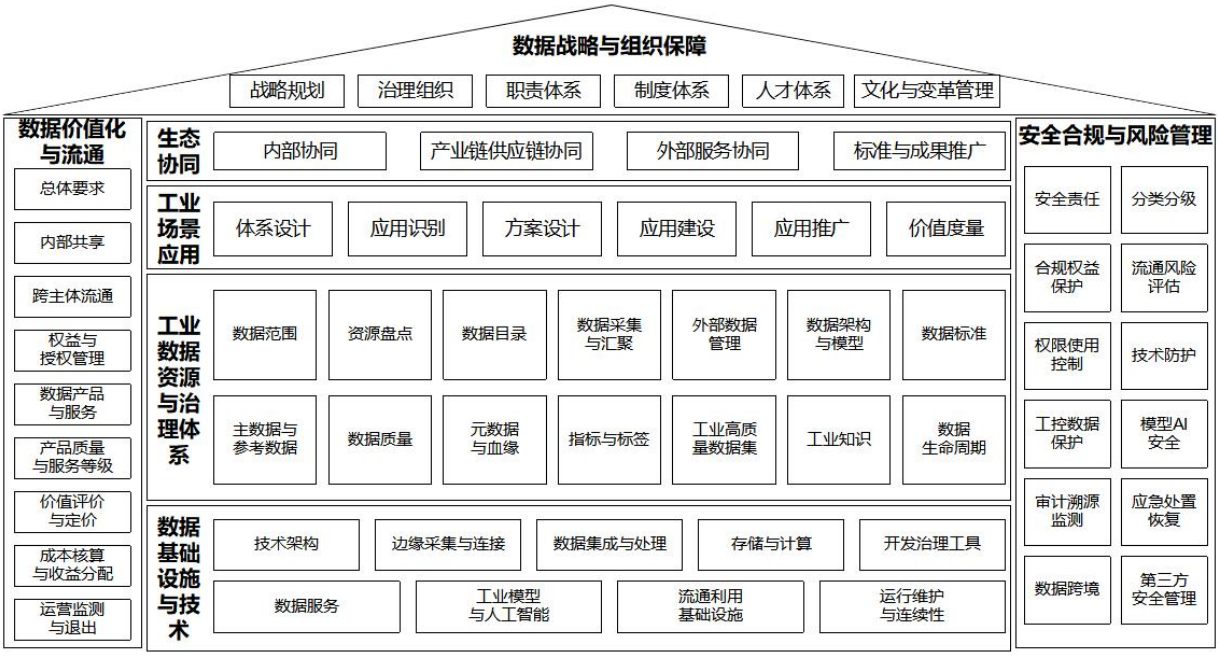


图 1 工业数据要素型企业建设总体框架

企业宜建立“需求识别—数据准备—能力建设—场景验证—运营评价—持续改进”的建设闭环。业务部门提出需求并确认价值目标，数据与技术部门完成数据和能力供给，安全与合规部门实施全过程审查，运营部门跟踪使用成效。建设闭环宜通过统一任务台账和指标体系进行管理，使场景、数据、模型、服务、责任和成效之间可关联、可追溯。

6 数据战略与组织保障

企业宜建立与数据要素建设范围相适应的战略、组织、职责、制度、投入、人才和文化保障。

6.1 战略规划

企业宜结合行业趋势、业务战略、数字化基础和数据资源特点制定中长期规划，并形成年度任务。规划宜包括现状与差距、建设目标、重点场景、能力布局、实施路线、资源投入、预期成效和风险控制。

规划宜与研发、生产、质量、设备、供应链、营销、服务、信息化和安全等专项规划衔接，并建立年度复盘和滚动调整机制。

6.2 治理组织

企业宜建立由主要负责人统筹，业务、数据、技术、安全、法务、财务、审计等部门参与的数据要素治理组织。具备条件的企业可设置首席数据官或同等职责岗位。不设置首席数据官的企业，应明确数据要素建设的分管负责人。

治理组织宜设置决策、协调、执行和监督层级，形成重大事项决策、跨部门协同、问题升级、风险处置和争议解决机制。

6.3 职责体系

企业宜明确数据所有者、数据管理者、数据提供方、数据使用方、数据产品负责人、平台运营方和安全管理方等角色。职责宜细化到数据对象、系统、场景和流程，覆盖标准制定、质量治理、权限审批、产品运营、安全保护、效果评价和问题整改。关键职责发生变更时宜及时更新并完成交接。

6.4 制度体系

企业宜建立由基本制度、管理办法、实施细则和操作指引构成的制度体系，覆盖数据采集、登记、治理、开发、共享、开放、流通、使用、归档和销毁。

制度宜明确适用范围、责任主体、审批权限、控制要求、记录留存和监督检查，数据要素相关考核、追责机制，并与企业现有业务、财务、采购、合同、知识产权、信息安全和保密制度衔接。

6.5 人才体系

企业宜配置数据架构、数据治理、工业知识、算法模型、数据产品、合规安全和运营管理等专业人员，建立岗位能力要求、分层培训、实践认证和人才发展机制。

6.6 文化与变革管理

企业宜通过管理层倡导、制度宣贯、场景共创、经验交流和激励约束，形成按标准生产数据、依数据开展决策、对数据质量负责的文化。

对涉及组织职责、业务流程、岗位操作和绩效方式变化的项目，宜制定变革计划，识别受影响人员，开展沟通培训、上线支持和使用反馈。

7 工业数据资源与治理体系

企业宜构建覆盖数据识别、采集、汇聚、组织、治理、使用和退出全过程的工业数据资源与治理体系，并建立与之相适应的治理组织、制度规范、流程机制和平台工具支撑。

7.1 数据范围

数据范围宜覆盖产品和服务运营管理全生命周期，包括研发、生产、供应链、销售、服务等欢姐内部数据，以及依法依规获取的公共数据、行业数据和合作方数据。

企业宜识别结构化、半结构化、非结构化、时序和空间数据等各类数据的不同形态，并明确实时性、精度、保留期限、安全等级和使用边界。

7.2 资源盘点

企业宜按业务域、系统、设备、组织和场景开展数据资源盘点，形成资源清单。盘点内容宜包括名称、业务含义、来源、责任主体、更新频率、存储位置、格式、质量、安全级别、共享范围和保留期限，并补充数据量级与使用状态。

资源盘点宜与信息系统、设备资产、接口、报表、算法模型和数据服务进行交叉核验，识别重复建设、数据孤岛、质量缺陷和权责不清等问题，盘点结果宜与数据目录联动并动态维护。

7.3 数据目录

企业宜按照全量覆盖、统一描述、动态更新和权责明确的原则建立工业数据目录，将数据资源、数据产品、数据服务、指标、标签、模型和接口纳入统一管理。

目录宜支持检索、申请、授权、调用、评价和追溯，并与业务流程、系统、设备、数据标准、质量规则和安全分类分级结果关联，目录信息宜与资源盘点清单保持一致。

7.4 数据采集与汇聚

企业宜根据场景需求确定采集范围、粒度、频率和时效，通过传感器、控制系统、工业软件、业务系统和标准接口等方式采集数据。采集应遵循合法、正当、必要原则，具有明确目的和合法依据，不宜重复采集或超范围采集。

企业宜建立批量、实时和边缘采集能力，规范设备、产线、车间、工厂和企业各层级数据接入，记录来源、时间、链路和处理过程，并对采集质量进行监测与异常告警。汇聚宜实现跨层级、跨系统共享复用，避免重复存储和数据口径不一致。

7.5 外部数据管理

引入外部数据前，企业宜明确业务用途、来源渠道、授权范围、质量要求、更新机制、费用、安全级别和退出条件，并对提供方资质与数据来源合法性进行必要核验。

外部数据宜与内部数据分别标识，保留采购、授权、交付和使用记录。应对外部数据开展合规风险评估，涉及公共数据的应符合公共数据开放共享相关规定。来源、授权或质量发生重大变化时，宜暂停使用并重新评估。

7.6 数据架构与模型

企业宜依据业务架构建设主题域、概念模型、逻辑模型和物理模型，明确工业对象、属性、关系和数据流向。

模型宜体现产品、物料、设备、工艺、组织、客户、供应商等核心对象之间的关联，并与系统建设和数据服务开发同步维护，模型变更需经过评审并保持版本可追溯。

7.7 数据标准

企业宜建立与业务标准、技术标准和安全标准衔接并符合国家和行业相关标准要求的数据标准体系，统一数据元、代码集、主数据、指标、标签、模型、接口和交换格式。

标准宜嵌入业务流程、系统建设、设备接入和数据产品开发过程，并建立提出、评审、发布、执行、变更、检查和废止机制。

7.8 主数据与参考数据

企业宜对产品、物料、设备、工艺、组织、客户、供应商等关键对象实施主数据统一管理，对状态、类型、地区、计量单位等公共代码实施参考数据管理。

宜明确权威来源和维护责任，建立申请、审核、发布、分发、变更和质量校核机制，减少一物多码、一名多义和跨系统不一致。系统新建或改造时，需同步开展主数据清洗、映射与迁移。

7.9 数据质量

企业宜建立覆盖源头、采集、传输、加工、存储、服务和使用的全过程质量管理机制，依据场景确定完整性、准确性、一致性、及时性、唯一性和有效性等指标，并对关键数据实施质量分级管理。

宜开展质量规则配置、自动监测、问题发现、责任分派、整改验证和效果评价，对关键问题实施根因分析和源头治理。质量结果宜与数据目录、产品说明和服务等级关联，并定期发布质量报告。

7.10 元数据与血缘

企业宜统一管理业务元数据、技术元数据和管理元数据，建立数据从来源到加工、产品服务及应用结果的血缘关系。

血缘宜支持影响分析、问题定位、变更管理、质量追溯和安全审计。关键数据加工逻辑和接口变更时，应同步更新元数据。

7.11 指标与标签

企业宜统一业务指标的名称、定义、口径、计算逻辑、维度、频率、责任主体和适用范围，建立指标发布和变更机制。建设统一指标库，实现指标统一取数和分级授权。

标签建设宜明确对象、来源、规则、有效期和使用限制，避免重复标签、不可解释标签和未经授权的敏感标签。建立标签创建、审核、使用、评估和下线全生命周期管理机制。

用于人工智能模型训练的高质量工业数据集，还应记录数据集偏见、局限性、已知缺陷。

7.12 工业高质量数据集

企业宜面向重点场景建设高质量工业数据集，明确用途、样本范围、标注规则、质量指标、版本、适用边界和安全要求。

数据集宜融合工业机理、业务规则和专家经验，建立样本代表性检查、标注一致性检查、偏差识别、版本更新和使用反馈机制。用于模型训练的数据集还宜记录训练、验证和测试划分，并留存抽样方法和划分依据。涉及个人信息或重要数据的数据集，需在使用前开展合规与安全评估。

7.13 工业知识

企业宜将工艺规则、设备机理、质量经验、故障案例、操作规范和专家经验等隐性知识进行规范化采集与结构化表达，建设知识库、规则库、案例库或知识图谱。

工业知识宜记录来源、责任人、适用对象、适用条件、验证状态和有效期，并通过专家评审、业务验证和使用反馈持续更新，建立知识采集、审核、发布、应用、评价和退役的全生命周期管理机制。

7.14 数据生命周期

企业宜依据业务价值、法律法规、合同约定和安全要求，对数据的创建、使用、变更、归档、迁移、备份、保留和销毁进行管理。对具有档案价值的工业数据，销毁前应按照档案管理法律法规开展档案鉴定，不得直接销毁属于档案的数据。

宜制定分类保留策略，识别失效、冗余和无主数据，备份宜定期开展恢复演练与有效性验证。销毁前应完成审批和影响评估，销毁过程应可验证、可记录。

8 数据基础设施与技术体系

企业宜建设与工业数据特征、业务连续性和安全要求相适应的数据基础设施与技术体系。

8.1 技术架构

企业宜构建衔接工控系统与工业互联网的分层架构，统筹边缘-工厂-企业全链管控，明确接口与安全域，以低时延高可靠能力从源头规避数据孤岛。

a) 企业宜形成与工业互联网平台、企业信息化系统和自动化控制系统衔接的数据技术架构，统筹边缘侧、工厂侧和企业侧的数据采集、传输、存储、计算、治理、服务和全生命周期安全能力，

适配工业现场毫秒级低时延、高可靠、强确定性的生产控制要求。

b) 架构宜明确组件边界、数据流向、接口关系、部署方式、扩展机制和安全域，同步配套异构协议兼容适配、跨平台数据迁移规则，避免形成新的平台孤岛。

8.2 边缘采集与连接

企业应构建安全可靠的边缘数据采集体系，在保障生产系统稳定运行的前提下，提升多源异构数据接入与边缘处理能力。

a) 企业宜支持工业协议解析、设备连接、边缘计算、断点续传、缓存补传、时间同步和采集状态监测，并对采集配置和设备身份进行管理。

b) 对生产控制敏感的数据，宜根据最小必要原则确定采集范围和传输路径，防止采集活动影响生产系统稳定运行。

8.3 数据集成与处理

企业宜构建多模态集成能力，强化处理过程全量留痕，支撑数据流转可控与可信。

a) 企业宜具备批量、实时、消息和文件等多种集成能力，对数据接入、转换、清洗、关联、汇总和分发任务实施统一编排。

b) 数据处理过程宜保留规则、参数、版本、运行日志和异常记录，支持任务重跑、结果校核和影响分析。

8.4 存储与计算

企业宜统筹存储选型、弹性计算调度与湖仓池一体架构，实现多源异构数据统一治理与存算协同，并通过容灾备份机制保障关键数据可恢复，满足业务连续性与安全合规要求。

a) 存储选型：企业宜根据数据类型、访问频率、保留期限、时效要求和成本效益，统筹选择关系型数据库、时序数据库、对象存储、数据仓库或数据湖等存储方式。

b) 计算调度：计算资源宜支持弹性扩展、资源隔离、负载调度和成本计量。构建分级存储体系，热数据保障低时延，温冷数据采用低能耗介质降本。

c) 湖仓池架构：企业宜依托湖仓池一体架构，实现多源异构数据统一治理，支持存算网协同与异构算力接入；重要数据需采用校验及密码技术保障安全。

d) 容灾备份：关键数据和服务宜具备备份、容灾和恢复能力，恢复时间目标与恢复点目标应满足业务连续性要求。

8.5 开发治理工具

企业应构建集成数据建模、质量管控、元数据管理与动态脱敏等能力的全生命周期治理工具链，依托统一权限与血缘解析强化标准落地，满足SJ/T 12131—2026及GB/T 36073合规要求，以流程自动化降低治理成本。

a) 工具能力：企业宜提供数据建模、标准管理、目录管理、质量管理、元数据管理、开发调度、分析建模和安全管理等工具，支持流程配置、版本管理、自动检查、问题工单和使用统计，并通过统一身份和权限体系进行控制。降低重复人工操作和治理成本。

b) 工具链建设：企业宜构建覆盖数据全生命周期的开发治理工具链，兼容多类存储形态，具备资产目录构建、血缘解析等核心能力，满足 SJ/T 12131—2026 要求。

c) 合规要求：工具宜符合 GB/T 36073 数据管理能力成熟度要求，强化数据标准落地与质量闭环管控，支持分类分级、敏感数据识别与动态脱敏。

8.6 数据服务

企业宜通过标准化封装数据服务，落实分类分级与全生命周期管控，依托加密传输、确权溯源与流通监测机制，保障服务合规可信，支撑数据要素价值评估与资产化管理。

a) 服务封装：企业宜将可复用的数据能力封装为数据集、接口、指标、标签、模型或应用服务，明确服务目录、申请条件、服务等级、版本、调用限制和责任边界，宜具备注册、发布、检索、申请、审批、调用、监控、计量、评价和下线等全生命周期管理能力，并为调用方提供清晰的说明文档和变更通知。
b) 合规流通：服务封装应落实分类分级要求，建立质量可验、来源可溯机制，界定使用许可与权责，保障合规可信。
c) 安全与确权：接口传输应采用加密与防篡改技术；服务宜与资产管理制度衔接，实现数据确权、成本核算及流通监测，支撑数据要素价值评估。

8.7 工业模型

企业应建立模型全生命周期管理机制，开展模型溯源与多维验证。跨主体联合建模宜采用隐私计算技术，确保工业智能应用安全可控。

a) 模型管理：企业宜建设覆盖模型开发、训练、验证、发布、监控、更新至退出的全生命周期管理体系，建立模型元数据管理机制，明确模型来源、训练数据、版本、适用场景、性能指标和责任主体，确保模型资产可审计、可溯源。
b) 应用验证：工业人工智能应用宜结合机理模型、业务规则和数据模型，开展准确性、鲁棒性、可解释性及业务适用性验证，未经充分验证的模型，不得直接用于关键生产控制。
c) 数据合规：模型训练数据宜基于高质量数据集，跨主体联合建模应采用隐私计算等技术实现数据安全保障，并按 GB/T 22239 等相关标准要求实施分级防护。

8.8 流通利用基础设施

企业应依托隐私计算与可信数据空间等技术底座，落实工业数据分级管控与全链路可信，通过参与基础设施互联互通与生态协同，实现安全合规下的数据价值释放与全要素生产率提升。

a) 技术支撑：企业开展跨主体数据流通利用时，根据风险和业务需求，宜采用可信数据空间、隐私计算、数据沙箱、区块链、数字水印和数据使用控制等技术；参与行业或国家数据基础设施互联互通时，宜遵循统一目录标识与接口规范。
b) 分级管控：企业宜建立工业数据分级管控机制。对高敏感数据宜采用“原始数据不出域、数据可用不可见”原则，采用隐私计算等技术实现过程可控、结果可计量，统筹安全合规与价值释放。
c) 能力建设：企业基础设施宜具备可信管控、价值共创与互联互通支撑能力，依托身份鉴权与数字合约实现全链路可信。
d) 生态协同：企业宜发挥链主作用，参与行业可信数据空间建设，推动产业链全环节数据共享与业务协同，提升全要素生产率。

8.9 运行维护与连续性

企业宜建立全链路监控与运维机制，落实关键服务等级与恢复目标，通过常态化演练审计保障业务连续性。

a) 企业宜对数据任务、接口、服务、算法模型和基础设施实施统一监控，建立容量管理、变更发布、故障处置、性能优化和服务连续性机制。

b) 宜制定关键服务等级和恢复目标，定期开展备份有效性验证、容灾切换、应急演练及业务连续性审计。

9 工业数据要素场景应用

企业宜以工业场景为数据要素价值释放的主要载体，形成从场景识别到运行推广的闭环。

9.1 体系设计

企业宜围绕研发设计、生产制造、经营管理、客户服务和产业协同构建场景体系，并根据行业特点补充专业场景。场景宜关联业务目标、流程环节、数据对象、模型能力、系统功能、责任主体和价值指标。

9.2 应用识别

企业宜通过战略分解、业务访谈、流程分析、问题工单、数据分析和对标研究识别场景，形成统一场景池。场景描述宜明确现状问题、目标用户、业务边界、关键决策、所需数据、预期价值和主要风险，避免以单一技术或产品替代业务场景。

企业宜从战略匹配度、业务价值、数据基础、技术可行性、实施成本、安全风险（包括合规风险）和推广潜力等方面评价优先级。宜优先选择价值明确、数据可得、责任清晰和风险可控的场景开展试点，并对高价值但基础不足的场景制定数据和能力补齐计划。

9.3 方案设计

场景方案宜明确业务流程、用户角色、功能需求、数据清单、数据处理规则、模型或算法、系统接口、安全边界、验收指标和运行机制。

方案宜区分业务规则、工业机理和算法模型的作用边界，对关键决策保留人工确认、异常处置和结果追溯机制。

9.4 应用建设

场景建设宜遵循“采、集、用”路径，规范采集所需数据，开展清洗、标注、融合、存储和知识化治理，形成数据集。

模型训练和验证宜使用已建设的高质量数据集，记录数据版本、参数、性能、限制条件和验证结果。

企业宜在试验环境或限定范围内开展功能、性能、数据质量、安全和业务成效验证，并设置与现状基线可比较的验收指标。涉及生产安全、质量判定、设备控制和人员权益的场景，应开展专项风险评估，明确人工干预和回退措施。

9.5 应用推广

场景上线后宜监测数据、模型、接口、业务流程和用户使用情况，建立异常反馈、问题处置、模型更新和版本发布机制。

推广前宜提炼标准、数据集、模型、接口、流程和实施模板，评估不同工厂、产线、产品和区域之间的差异，不宜简单复制。

9.6 价值度量

企业宜建立场景基线并设置可量化指标，评价对研发周期、生产效率、产品质量、设备可靠性、能源消耗、运营成本、客户体验、供应链韧性和安全水平的影响。价值评价宜同时考虑建设投入、运营成

本、风险成本、应用范围和持续时间，避免仅以单次试点效果代替长期价值。

表 1 场景优先级评价维度示例

评价维度	内容
战略匹配度	与企业战略、年度重点任务的关联程度
业务价值	提质、增效、降本、绿色、安全、创新效果
数据基础	数据可得性、质量、时效、权责和合规条件
技术可行性	技术成熟度、集成复杂度、运行稳定性
实施成本	建设周期、投资、人员和运维成本
安全风险	数据、生产、模型、个人信息和供应链风险、合规风险
推广潜力	跨产线、工厂、产品和产业链复用能力

10 数据价值化与流通机制

企业宜建立覆盖供需对接、授权使用、产品服务、价值评价、收益分配和运营退出的数据价值化与流通实现机制。

10.1 总体要求

数据流通利用应具有明确目的、合法来源、清晰边界和必要安全措施。企业宜根据数据风险、主体关系和使用方式选择内部共享、协议提供、产品服务或可信环境计算等模式。

流通过程宜做到需求可登记、数据可识别、授权可验证、使用可控制、操作可审计、结果可评价、责任可追溯。

10.2 内部共享

企业宜通过统一目录和服务渠道实现按需共享，建立需求提出、可用数据发现、申请审批、交付调用、异议处理和服务评价机制。

对高频共性需求宜沉淀标准数据服务，减少点对点接口和重复加工。共享数据发生口径、质量、权限或服务变更时，宜及时通知使用方。

10.3 跨主体流通

企业与外部主体开展数据流通前，应识别数据类别和级别，核验来源与授权基础，评估目的、范围、方式、期限和安全风险。涉及重要数据、个人信息流通的，应依法开展风险评估、履行法定程序。

数据提供方应确保来源合法并明确使用要求；数据接收方应按照约定使用，不应超范围使用或向未授权第三方提供；平台或服务方应按照约定履行技术和安全职责。

10.4 权益与授权管理

企业宜识别数据持有、加工处理和产品经营等活动中的相关权益和义务，通过协议、授权书、管理要求等方式明确使用范围。

授权内容宜包括数据对象、目的、方式、对象、地域、期限、再提供限制、成果权益、保密义务和退出要求。授权发生变更或终止时，宜同步调整权限和数据处理状态。

10.5 数据产品与服务

企业宜围绕稳定需求开发数据集、接口、报告、指标、标签、模型、应用和专业服务，形成需求分析、产品设计、合规审查、开发测试、发布交付、运营监测、客户反馈和退出流程。产品说明宜明确内容、来源、加工方式、质量、适用范围、使用限制、更新频率、安全级别、服务等级和责任边界。

企业宜为数据产品设置准确性、完整性、及时性、稳定性和一致性等质量指标，为数据服务设置可用性、响应时间、处理时限、支持方式和故障恢复等服务等级。宜建立质量监测、服务报告、问题响应、补救措施和变更通知机制。无法达到约定时，应按合同或服务规则处理。

10.6 价值评价

企业可综合数据形成成本、治理成本、稀缺程度、质量水平、使用范围、更新频率、场景贡献、替代成本和风险成本开展价值评价。开展定价与价值评价不得损害国家利益、社会公共利益，不得实施垄断行为。

定价宜与产品形态、服务等级、授权范围和使用期限相匹配，可采用固定费用、按量计费、订阅、效果分成或组合方式，并保留评价和定价依据。

10.7 成本核算与收益分配

企业宜识别数据采集、治理、平台、模型、安全、交付和运营等成本，建立可追溯的成本归集口径。

涉及多部门或多主体共同贡献时，宜依据数据贡献、加工贡献、场景贡献、资源投入和风险承担等因素约定收益分配。相关活动应符合适用的财务、税务、会计和法规的要求。

10.8 数据产品运营监测

企业宜监测需求响应、调用量、活跃用户、复用范围、质量达标、服务等级、运营成本、收益和安全事件等情况，定期评价产品服务的持续价值。

当数据来源失效、授权终止、质量不达标、风险不可接受或长期无使用时，宜按程序下线产品服务，通知相关方并完成数据返还、删除、归档或匿名化处理。

11 安全合规与风险管理

企业应统筹发展与安全，将安全合规要求贯穿工业数据供给、流通、使用和销毁全过程。

11.1 安全责任

企业应落实数据安全主体责任，建立覆盖决策、管理、执行和监督的责任体系，明确主要负责人、数据安全负责人、业务部门、技术部门和使用人员职责。安全责任宜纳入岗位说明、项目流程、合同协议和绩效检查，对重要事项建立审议、报告和问责机制。

11.2 分类分级

企业应按照 GB/T 43697—2024 及适用行业要求开展数据分类分级，形成目录并实施动态管理。对重要数据，应按照国家有关规定进行识别、申报并落实保护要求。企业宜根据类别、级别、场景、范围和接收方能力配置差异化措施。重要工业数据识别应结合行业主管部门发布的重要数据目录开展。

11.3 合规与权益保护

企业应识别数据采集、持有、使用、加工、传输、提供、公开、删除和跨境等活动的合规要求，建立合规清单、审查流程和记录留存机制。处理个人信息、商业秘密、知识产权和受合同限制的数据时，应落实相应权益保护，不应通过强迫、欺诈、误导等方式取得授权。

11.4 流通风险评估

企业宜在数据流通前评估数据敏感程度、使用目的、接收主体、处理环境、流通方式、关联分析、再提供和退出等风险。评估结果宜明确允许流通的数据范围、必要的脱敏或匿名化处理、技术环境、访问限制、审计要求和应急安排。高风险事项宜提交专门审议。

11.5 权限与使用控制

企业宜实施统一身份管理、强身份鉴别、最小权限、职责分离和定期复核，对高风险操作设置二次确认或多人审批。权限宜与人员、岗位、项目、场景、数据级别和期限关联。人员离岗、合作终止或用途变化时，应及时调整或收回权限。

11.6 数据安全防护

企业宜按照风险实施加密传输、加密存储、脱敏、匿名化、防泄漏、接口防护、终端管控、备份恢复和安全监测等措施。安全措施宜经过测试验证并纳入变更管理。密钥、证书、脱敏规则和安全策略应由授权人员管理，防止长期不变或失效。

工业控制系统与企业数据平台之间宜实施分区分域、边界防护和受控交换，避免数据采集、分析或外部服务影响生产控制稳定性。涉及工艺参数、控制指令、设备状态和安全联锁的数据，应严格限制访问、修改和外发，并对远程运维和跨网交换实施专项控制。

11.7 模型安全防护

企业宜识别训练数据泄露、模型窃取、对抗输入、输出失真、偏差放大和不当自动决策等风险，建立模型安全测试和运行监测。模型输出用于关键生产、质量、安全或人员管理时，宜设置业务规则约束、人工复核、异常告警和回退机制。

11.8 审计溯源与监测

企业宜记录数据访问、下载、加工、导出、共享、授权、模型调用和管理操作，确保日志时间一致、内容完整、留存适当并防止篡改。可采用技术增强溯源能力。宜持续监测异常访问、批量导出、越权使用、数据泄露和服务中断风险。

11.9 应急处置与恢复

企业宜制定数据安全事件应急预案，明确事件分级、报告路径、处置权限、证据保全、业务恢复、外部协同和改进要求。宜定期开展演练。发生事件时，应及时止损、调查、报告、恢复和复盘，并根据原因更新技术、流程、合同或人员管理措施。

11.10 数据跨境

涉及数据跨境时，企业应识别适用法律法规和监管要求，明确数据范围、目的、接收方、存储地点、后续处理和安全措施，并依法履行相应程序。重要数据、个人信息出境，应当依法开展数据出境安全评估等法定程序。企业宜建立跨境数据台账和持续监督机制，对接收方变更、用途变化、再转移和安全事件进行管理。

11.11 第三方机构安全管理

企业宜对数据平台、云服务、开发运维、安全服务和数据处理等对第三方机构开展准入评估，合同中明确数据处理、安全保护、审计、事件报告、分包、退出和违约责任。宜持续监测第三方机构履约和安全状况；合作结束后，应回收账号权限，核验数据返还、迁移或删除结果。

12 数据生态协同

企业宜以平等、自愿、互利和安全为基础，与内外部主体开展工业数据要素协同。

12.1 内部协同

企业宜建立信息技术、研发、业务和生产部门之间的数据协同机制，明确统建能力和共享服务边界。跨部门场景宜由业务和数据共同负责，形成需求、数据、模型、系统、安全和运营一体化团队。

12.2 产业链供应链协同

企业宜与上下游企业共同制定数据接口、主数据、产品编码、质量追溯和协同业务规则，促进设计、计划、质量、库存、物流和服务数据可信流通。宜按照贡献和风险合理约定使用权益和收益。

12.3 外部服务协同

企业可与工业互联网平台、数据商、数字化转型服务商、数据安全服务机构、数据交易场所和第三方评估机构合作。宜对服务机构的专业能力、安全能力、服务连续性和履约情况进行评价，并避免对单一技术路线或供应商形成不可控依赖。

12.4 成果推广

企业宜将成熟实践转化为企业标准、团体标准、行业标准或国家标准，形成可复制的方法、工具、数据集和案例。对外发布案例和成果前，应开展数据、商业秘密、知识产权和宣传合规审查，不宜披露可识别敏感信息或未经验证的成效。

13 数据要素效能评价与改进

企业宜建立与建设目标相匹配的评价与持续改进机制，以客观评价校验目标实现程度，牵引能力建设不断迭代提升。

13.1 评价机制

企业可参考 GB/T 36073—2025与GB/T 37988—2019，选用自评价、内部审计、用户评价或第三方评价等路径。评价周期宜与规划节奏、关键项目节点、重大变更及风险态势相协调；评价组织宜保持必要的独立性与专业能力。

13.2 评价指标

评价指标宜涵盖战略组织、数据资源、数据治理、技术支撑、场景应用、流通运营、安全合规、生态协同及实施保障等维度，示例见附录 C。

附录 C 指标为资料性示例，企业可根据自身行业、规模、发展阶段删减、调整指标。各项指标宜具备清晰的名称、定义、口径、来源、周期、目标值与责任主体；企业可结合自身行业、规模与所处阶段设定差异化指标。

13.3 评价实施

评价宜优先采信系统日志、监控记录、业务台账与财务凭证等可追溯数据；定性评价应留存制度、流程、报告、访谈及现场检查等佐证。采用抽样时宜界定样本范围、抽样方法与统计区间，并对异常值与缺失值作出说明；评价数据的采集与使用应符合安全保密和个人信息保护要求。

评价宜依次开展准备、取证、算值、综合研判、结果确认与报告发布；跨单位或跨场景评价宜统一口径与基准。评价结果宜厘清事实、判断与改进建议；存在争议的事项宜保留依据与处置记录。

13.4 评价结果与改进

企业宜将评价结论用于规划修编、项目决策、预算安排、场景推广、产品打磨、风险整治与人员培训。不宜仅凭单一指标判定建设成效；对短期难量化但具战略价值的基础能力，宜结合长期运行与复用表现综合评判。

企业宜依据评价结论建立问题与改进台账，明确优先级、责任方、时限、资源需求与验证手段。对反复出现或影响严重的问题宜做根因剖析，从制度、流程、标准、平台、模型或人员能力等层面加以改进，并跟踪落地后的真实成效。

附录 A

（资料性）

评价指标示例

表 A.1 给出了评价指标示例。企业宜结合行业属性、业务目标和建设阶段确定指标口径、目标值和统计周期。

表 A.1 评价指标示例

评价领域	指标名称	参考口径	主要证据
战略组织	规划任务完成率	按期完成任务数/计划任务数	计划与验收记录
战略组织	职责覆盖情况	关键角色和数据对象责任明确程度	职责清单、岗位说明
战略组织	制度执行情况	制度检查问题及整改完成情况	检查与整改记录
战略组织	专业人员保障	关键岗位配置和能力达标情况	人员和能力评价记录
数据资源	目录覆盖率	已纳入目录资源数/应纳入资源数	资源盘点和目录记录
数据资源	目录更新及时率	按要求及时更新目录项占比	目录变更日志
数据治理	标准执行率	符合标准的数据项或接口占比	标准检查报告
数据治理	关键数据质量达标率	达到质量目标的关键数据项占比	质量监测报告
数据治理	质量问题闭环率	完成整改并验证的问题占比	质量工单
数据治理	血缘覆盖率	建立端到端血缘的关键数据占比	血缘平台记录
数据治理	高质量数据集复用度	使用数据集的场景或模型数量	调用和使用记录
技术支撑	数据服务可用率	服务正常时间/应服务时间	监控报告
技术支撑	接口响应达标率	满足服务等级的调用占比	接口监控日志
技术支撑	数据任务成功率	成功完成任务数/执行任务数	调度日志
技术支撑	故障恢复达标率	在目标时间内恢复的故障占比	故障和恢复记录
场景应用	场景上线完成率	按计划上线场景数/计划数	项目和上线记录
场景应用	场景活跃使用率	持续活跃使用场景占比	用户与访问记录
场景应用	业务指标改善度	上线前后核心业务指标变化	基线和业务数据
场景应用	场景复制推广数	完成跨单位或跨产线推广数量	推广和验收记录
流通运营	需求响应及时率	在承诺时间内响应需求占比	需求工单
流通运营	数据产品复用率	被多个用户或场景使用的产品占比	产品调用记录
流通运营	服务等级达标率	达到约定服务指标的周期占比	服务报告
流通运营	产品运营贡献	产品服务收益或内部价值贡献	运营与财务记录
安全合规	分类分级覆盖率	完成分类分级的数据资源占比	分类分级目录
安全合规	权限复核完成率	按期完成复核的权限占比	权限复核记录
安全合规	高风险问题整改率	完成整改并验证的高风险问题占比	风险和整改台账

安全合规	安全事件处置达标率	按预案及时处置的事件占比	事件报告
生态协同	协同主体覆盖	参与数据协同的内外部主体数量	合作和调用记录
生态协同	标准化成果	形成或参与制定的标准、规范数量	标准成果材料
持续改进	改进任务完成率	按期完成改进任务数/计划数	改进台账

参 考 文 献

[1] 20255407-T-907 数据 基础术语
[2] GB/T 48560-2026 高质量数据集 数据标注要求
[3] GB/T 38667—2020 信息技术 大数据 数据分类指南
[4] 中共中央、国务院.关于构建数据基础制度更好发挥数据要素作用的意见. 2022 年.
[5] 国家数据局等 17 部门.“数据要素×”三年行动计划（2024—2026 年）. 2023 年.
[6] 工业和信息化部办公厅.工业场景数据要素应用参考指引（2025 年版）.
[7] 中华人民共和国数据安全法
[8] 中华人民共和国网络安全法
[9] 中华人民共和国个人信息保护法