工业领域数据安全能力提升实施方案
（2024–2026 年）

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通等各环节，保障数据安全，事关国家安全大局。为贯彻落实习近平总书记关于数据安全的重要指示精神和党中央、国务院决策部署，推动《中华人民共和国数据安全法》《中华人民共和国网络安全法》《工业和信息化领域数据安全管理办法（试行）》等在工业领域落地实施，加快提升工业领域数据安全保护能力，助力工业高质量发展，夯实新型工业化发展的安全基石，制定本方案。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大精神，坚定不移贯彻总体国家安全观，坚持统筹发展和安全，坚持底线思维和极限思维，坚持目标导向和问题导向，以构建完善工业领域数据安全保障体系为主线，以落实企业主体责任为核心，以保护重要数据、提升监管能力、强化产业支撑等为重点，提高数据安全治理能力，促进数据要素安全有序流动和价值释放，为加快推进新型工业化，建设制造强国、网络强国和数字中国提供坚实支撑。

（二）基本原则

统筹推进，重点突破。加强顶层谋划，系统推进数据安全组织架构、政策制度、管理机制、标准规范、技术手段建设和产业发展工作。以强化重点行业、重点企业、重要系统平台、重要数据保护为切入点，以点带面促进整体保护水平提升。

政府引导，协同共治。综合运用正向激励和反向约束等方式，选树标杆典型，强化监管执法，压实企业主体责任。充分发挥行业协会、龙头企业、专业机构、高等院校等各方力量，形成数据安全协同治理的良好局面。

场景牵引，分业施策。摸清数据处理重点环节风险易发场景的特点规律，紧贴业务场景数据保护需求，强化科学防控。结合行业特色、数据特征等，差异化指导、精准化施策，加速提升行业数据安全管理水平。

创新驱动，技管结合。不断创新管理模式、技术、产品与服务，适应新时期工业领域数据安全保护新形势、新特点和新需求。注重“以技管数”手段建设和运用，与日常监管形成合力。

（三）总体目标

到2026年底，工业领域数据安全保障体系基本建立。数据安全保护意识普遍提高，重点企业数据安全主体责任落实到位，重点场景数据保护水平大幅提升，重大风险得到有效防控。数据安全政策标准、工作机制、监管队伍和技术手段更加健全。数据安全技术、产品、服务和人才等产业支撑

能力稳步提升。

——基本实现各工业行业规上企业数据安全要求宣贯全覆盖。

——开展数据分类分级保护的企业超4.5万家，至少覆盖年营收在各省（区、市）行业排名前10%的规上工业企业。

——立项研制数据安全国家、行业、团体等标准规范不少于100项。

——遴选数据安全典型案例不少于200个，覆盖行业不少于10个。

——数据安全培训覆盖3万人次，培养工业数据安全人才超5000人。

二、重点任务

（一）提升工业企业数据保护能力

1.增强数据安全保护意识。加大数据安全法律法规和政策标准宣贯培训力度，提高各行业企业数据安全意识。督促企业依法依规落实数据安全主体责任，压实各单位法定代表人或主要负责人数据安全第一责任，建立健全数据安全管理体系和工作机制，配足数据安全岗位和人员队伍，定期开展数据安全教育培训。引导企业贯彻发展与安全并重原则，将数据安全管理要求融入本单位发展战略和考核机制，加强数据安全工作与业务发展同谋划、同部署、同落实、同考核。

2.开展重要数据安全保护。指导企业建立健全数据分类分级保护等安全管理制度，定期梳理识别重要数据和核心数

据，形成目录并及时报备。督促重要数据和核心数据处理者明确数据安全负责人和管理机构，落实数据分级防护要求，每年至少开展一次数据安全风险评估，及时发现整改安全隐患，按要求报送评估报告。指导企业加强重要数据和核心数据安全风险监测与应急处置，及时报告重大风险事件。推动各行业企业加强商用密码应用保护数据安全。

3.强化重点企业数据安全管理。遴选掌握关键核心技术、代表行业发展水平、关系产业链安全稳定或关乎国家安全的企业，滚动编制工业领域数据安全风险防控重点企业名录。将名录内企业作为数据安全监管重点，督促其在落实数据安全要求基础上，着重提升风险监测、态势感知、威胁研判和应急处置等能力。发挥部省两级主管部门作用，统筹各方数据安全监测预警手段和技术力量，加强技术支持，协同做好企业数据安全保护。

4.深化重点场景数据安全保护。指导企业围绕数据汇聚、共享、出境、委托加工等重点数据处理场景，排查数据安全保护薄弱点，实施贴合行业特点的数据保护措施。聚焦供应链上下游协作、服务外包、上云上平台等典型业务场景，厘清多主体数据安全责任界面和衔接模式，建立全链条全方位数据安全保护体系。针对勒索病毒攻击、漏洞后门、人员违规操作、非受控远程运维等易发频发风险场景，加强风险自查自纠，采取精准的管理和防护措施。面向数据要素大规模流通交易典型场景，打造一批安全解决方案。

专栏1　数据安全保护筑基工程
1.夯实数据分类分级基础。分行业分领域研究制定重要数据和核心数据识别细则，形成“1+N”的工业领域数据分类分级规范体系，科学指导各行业落地实施。持续迭代重要数据和核心数据目录，逐步摸清行业重要数据规模、分布、处理等情况，明确行业重点保护数据对象。 **2.编制数据保护实践指南。**结合重点数据处理场景、典型业务场景、易发频发风险场景等数据安全保护需求和难点，研究制定工业领域数据安全保护实践系列指南，为企业数据保护和风险防范提供实操参考。面向数据出境需求较大的重点行业，分类制定数据出境安全指引，指导企业依法依规开展数据出境安全评估。 **3.分业推进数据安全保护能力跃升。**在有序推进宣贯培训、分类分级保护等工作基础上，立足钢铁、汽车、纺织、集成电路等行业实际，聚焦重点场景、重点环节、重要系统平台、重要数据等，进一步加强行业数据安全主体责任落实和保护力度，实现行业数据安全保护能力整体跃升。

（二）提升数据安全监管能力

5.完善数据安全政策标准。建立健全工业领域数据安全管理制度，推动出台风险评估实施细则、应急预案、行政处罚裁量指引等政策文件。持续完善重要数据识别、备案、分

级防护、风险评估等全流程监管机制，加强监督检查。组建工业领域网络与数据安全行业标准化组织，发布数据安全标准体系建设指南，加快研制重要数据识别、安全防护、风险评估、产品检测、密码应用等亟需标准。鼓励地方参照制定本地区数据安全政策。

6.加强数据安全风险防控。完善工业领域数据安全风险信息报送与共享工作机制，组建数据安全风险分析专家组，动态管理风险直报单位库，协同加强地方力量，常态化开展风险监测、报送、预警、处置等工作。摸排数据安全风险事件特点和规律，建立重大风险事件案例库，加强案例剖析和风险提示。面向重点行业开展“数安护航”专项行动，定期组织“数安铸盾”应急演练，提升事件快速反应、规范处置、协同联动水平。

专栏 2　打造数据安全风险防控品牌
1.“数安护航”专项行动。分行业、分批次集中开展数据安全风险排查和防范，聚焦数据泄露、篡改、滥用、违规传输、非法访问、流量异常等突出风险，利用企业自查、远程检测、现场诊断等手段，针对性增强风险应对处置能力。 **2.“数安铸盾”应急演练。**面向重点行业，模拟勒索病毒攻击、供应链攻击等易发典型数据安全风险事件，组织开展全要素、全流程应急演练，持续优化事件响应流程和机制，锻炼培养一批应急支撑队伍。

7.推进数据安全技术手段建设。统筹建设工业和信息化领域数据安全管理平台，建立工业领域数据安全工具库，形成集数据资源管理、态势感知、风险信息报送与共享、技术测试验证、事件应急响应等功能于一体的技术能力，加强与网络安全技术、密码技术手段协同。推动有条件的地方、行业、企业等加快建立数据安全风险监测与应急处置等技术手段，强化“部-省-企业”技术能力三级联动，不断提升技术保障水平。

专栏3　数据安全技术保障工程
1.统筹建设工业和信息化领域数据安全管理平台。建立完善工业领域数据安全监测、信息报送与共享、应急管理、安全评估等系统功能，强化风险统一汇集、分析、研判和通报，支撑事件应急处置、辅助决策、跟踪追溯等工作，提供风险评估、出境安全评估、防护能力评估等服务，覆盖不少于20个省级（行业级）节点和500个企业节点。 **2.建立工业领域数据安全工具库。**围绕数据分类分级、安全防护、检测评估、合规检查、应急处置、攻击追溯、密码应用等方面，研发一批规范化、便携式的工具，为高效开展数据安全监管和保护工作提供支撑。

8.锻造数据安全监管执法能力。规范数据安全事件调查处置程序，丰富取证方法和手段。加快完善数据安全执法流程和工作机制，推动地方工业和信息化主管部门将数据安全

纳入本地区行政执法事项清单，指导各行业、各地方依法严格处置违法行为，加强执法案例宣介与警示教育。建立健全数据安全违法违规行为投诉举报机制，多渠道收集违法违规线索。加大监管执法人员培训力度，推动地方工业和信息化主管部门强化数据安全监管力量，打造专业化、规范化监管执法队伍。

（三）提升数据安全产业支撑能力

9.加大技术产品和服务供给。加强工业数据智能分类分级、工业数据库审计、低时延加密传输等共性技术优化升级。加大适配工业业务场景和数据特征的轻量级数据加密、隐私计算、密态计算等关键技术攻关。支持使用商用密码技术保障工业领域数据安全。围绕工业数据泄露、窃取、篡改等风险，推动流量异常监测、攻击行为识别、事件追溯和处置等产品研发。加强面向工业云、工业大数据、工业互联网平台等新兴应用的数据安全架构设计。支持工业领域数据安全“产品+服务”供给模式创新。

10.促进应用推广和供需对接。加大多方安全计算、数据防勒索、数据溯源、商用密码等技术产品在工业领域的试点应用。组织遴选一批在各行业具有广泛应用价值的通用数据安全技术和产品，打造一批面向行业、面向场景、面向中小企业的数据安全解决方案，形成一批工业领域数据安全典型案例，分行业、分地区开展宣传推广。推动各行业利用主题沙龙、路演等渠道开展数据安全技术产品和服务供需对接活

动。发挥数据安全产业公共服务平台作用，强化信息共享、资源对接等服务。

11.建立健全人才培养体系。面向不同行业、岗位、层级数据安全工作需求，推动专业化、特色化数据安全教材课程开发，规范化开展职业人才资格认定。支持产学研用各方加强合作，依托培训中心、实训基地、网络学习平台等联合培养复合型管理人才和实战型技能人才，通过技能竞赛、技术交流、学习进修、岗位练兵等形式持续促进人才知识更新和能力提升。鼓励工业企业建立健全数据安全绩效评价机制，加强数据安全人才激励。

三、保障措施

（一）加强组织协调。工业和信息化部加强工作统筹，做好与国家数据安全工作协调机制的衔接。各地工业和信息化主管部门负责组织实施本地区实施方案。鼓励各地结合实际制定细化工作方案，加强与相关部门合作，确保目标任务落实。充分发挥高校、科研院所、第三方机构等在实施方案宣贯、手段建设指导、技术交流合作、成果应用推广等方面的专业作用，引导企业加强数据安全能力建设。

（二）加大资源保障。统筹利用现有资金渠道，加大工业领域数据安全工作投入，支持关键核心技术攻关和公共服务平台建设。深化产融合作，支持数据安全企业参与“科技产业金融一体化”专项，通过国家产融合作平台获得便捷高效的金融服务。鼓励各地将数据安全纳入地方工业领域数字

化转型发展相关规划，在支持数字化、网络化、智能化等项目时，同步明确数据安全要求。引导企业在信息化建设中为数据安全防护安排一定比例资金。

（三）强化成效评估。各行业、各地区及时跟踪调度实施方案落实情况，总结经验做法，评估工作成效，加强沟通交流，及时报告重大进展情况或问题。工业和信息化部对工作推动有力、取得明显成效的地区、企业和单位予以表扬，对优秀经验做法加强提炼总结和推广应用。

（四）做好宣传引导。综合利用产业活动、国际合作等方式，宣传普及工业领域数据安全理念和举措，提高地方、企业和公众对工业领域数据安全的认可度。充分调动行业协会、学会、产业联盟等力量，引导企业加强自律、凝聚共识，营造行业数据安全保护良好氛围。