

工业和信息化部司局简函

工网安函〔2024〕340号

工业和信息化部网络安全管理局关于做好《工业领域数据安全能力提升实施方案（2024-2026年）》落实工作的函

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部门，有关中央企业，部内相关司局：

为加快推动落实《工业领域数据安全能力提升实施方案（2024-2026年）》（以下简称《实施方案》），按照部相关工作安排，现就有关事项通知如下：

一、请各地工业和信息化主管部门、各有关中央企业结合职责扎实推进以下工作：

1.填写《〈实施方案〉年度计划表》（模板见附件1），细化工作目标，提出落实举措，于2024年6月30日前将相关材料（盖章纸质版和电子版各1份）报我局。请结合计划安排，督促指导本地区、本集团数据处理者参照有关数据安全政策标准、工作指南等，规范化开展数据安全工作，切实履行数据保护责任和义务。

2.参照数据安全宣贯培训建议课程表（附件2），通过政策宣贯、专题培训、座谈研讨、产业活动等方式，加强数据安全相关法律法规政策解读、技能培训和宣传推广。

3.定期总结评估《实施方案》落实成效，通过数据安全工作简讯等形式及时将重点工作进展和经验做法报我局。

我局将汇总有关情况，以简讯合刊、案例分享等方式促进各方加强交流、推广经验。

二、请部内相关司局对照《实施方案》总体部署和工作要点，指导和督促本行业本领域数据安全工作，提升行业数据安全保护水平。

三、请各单位加大资源投入，加强工业领域数据安全工作支持。鼓励各单位将数据安全工作与“智改数转网联”、新一轮技术改造和设备更新、中小企业数字化转型等工作统筹考虑、同步推进。

特此通知。

附件：1.《工业领域数据安全能力提升实施方案
(2024-2026年)》年度计划表(模板)
2.数据安全宣贯培训建议课程表

工业和信息化部网络安全管理局

2024年6月4日

(联系人及电话：张洪 68206195/13911192293)

附件 1

《工业领域数据安全能力提升实施方案（2024-2026 年）》年度计划表（模板）

填报单位（加盖公章）：

联系人及电话：

一、《实施方案》量化指标分解（地方工业和信息化主管部门填报）									
序号	任务	年份	三年任务总目标	2024 年		2025 年		2026 年	
				完成情况	占比	完成情况	占比	完成情况	占比
1	实现本地区各工业企业行业规上企业数据安全要求全覆盖		（填写本地区各行业行业规上企业总数）						
2	开展数据分类分级保护的至少覆盖年营收在本地区行业排名前 10%的规上工业企业		（填写年营收在本地区行业排名前 10%的规上工业企业数量）						

3	累计推荐本地区数据安全典型案例不少于50个	(推荐典型案例总数)							
4	本地区数据安全培训累计覆盖不少于1000人次	(数据安全培训累计覆盖总人次)							
5	指导本地区企业建设数据安全风险评估等节点	(企业数据安全风险评估节点建设总数)							

二、《实施方案》2024年度重点任务落实举措（地方工业和信息化主管部门、有关中央企业填报）

序号	重点任务	具体工作举措	完成时间
1	增强数据安全保护意识		
2	开展重要数据安全保护		
3	强化重点企业数据安全的管理		
4	深化重点场景数据安全保护		
5	完善数据安全政策标准		
6	加强数据安全风险防控		

7	推进数据安全技术手段建设 ¹		
8	锻造数据安全监管执法能力 ²		
9	加大技术产品和服务供给		
10	促进应用推广和供需对接		
11	建立健全人才培养体系		
12	其他 ³		

¹ 请在该项任务落实举措中明确省级工业领域数据安全风险监测等技术能力建设的有关考虑，如已有工作基础请写明具体情况。

² 请在该项任务落实举措中明确将数据安全纳入本地区行政执法事项清单计划的有关考虑，如已有工作基础请写明具体情况。

³ 包括但不限于本地区、本集团开展的特色活动、工作举措等。

附件 2

数据安全宣贯培训建议课程表

序号	课程名称	课程主要内容
一、通识课程		
1	《工业和信息化领域数据安全管理办法（试行）》解读	概括介绍《数据安全法》及行业“1+5”政策体系，解读《工业和信息化领域数据安全管理办法（试行）》主要内容
2	《工业领域数据安全能力提升实施方案（2024-2026年）》解读	围绕《工业领域数据安全能力提升实施方案（2024-2026年）》目标、重点任务等进行解读，明确企业侧、监管侧、产业侧重点工作
3	工业领域重要数据识别、防护与评估	讲解工业领域重要数据识别和目录备案、分级防护、风险评估等要求和实操要点
4	工业领域数据安全风险防范与处置	讲解工业领域数据安全风险形势、风险信息报送与共享要求、典型风险防范与处置等内容
二、专题课程		
1	工业领域数据安全技术保障能力建设	讲解工业领域数据安全风险监测、信息共享、应急处置、安全评估等技术手段建设的思路框架和重点内容

2	工业领域数据安全行政执法	讲解工业领域数据安全行政执法形势、情形、流程、要求等内容
3	工业领域数据出境安全评估	讲解《数据出境安全评估办法》《促进和规范数据跨境流动规定》相关政策要点及工业领域数据出境安全评估实践等内容
4	工业领域数据安全典型案例分享	交流分享工业领域数据安全典型案例、优秀经验做法等内容
5	工信领域数据安全人才培养体系	讲解数据安全人才培养体系相关内容
6	《数据防勒索指南》解读	结合《数据防勒索指南》讲解当前数据勒索类型、传播方式、攻击流程，事前、事中、事后的防范措施等内容

工业和信息化部文件

工信部网安〔2024〕34号

工业和信息化部关于印发《工业领域数据安全能力提升实施方案（2024—2026年）》的通知

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部门，有关行业协会，有关企业，部属有关单位，部属各高校：

现将《工业领域数据安全能力提升实施方案（2024—2026年）》印发给你们，请认真抓好贯彻落实。

(此页无正文)



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

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（详见附件）。

（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要，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。

附件：部分行业数据安全保护能力跃升工作要点（仅发地方工业和信息化主管部门、部内相关司局）

附件

部分行业数据安全保护能力跃升工作要点

(仅发地方工业和信息化主管部门、部内相关司局)

在整体推进各地区、各行业数据安全工作基础上，首批面向钢铁、有色、石化化工、汽车、民机、民船、纺织、集成电路、软件等行业，形成如下工作要点。其他行业可参照制定本行业要点。

一、钢铁行业

(一) 工作目标

到 2026 年底，钢铁行业开展数据分类分级保护的规上工业企业超 100 家，数据安全宣贯培训覆盖 3000 人次，数据安全保护意识普遍提高；立项研制数据安全标准规范 5 项，分类分级、应用数据安全等关键标准供给能力显著增强；组织开展专项行动，加强数据安全风险排查与防范；遴选不少于 10 个数据安全典型案例，形成可复制可推广的行业实践模式。

(二) 重点任务

1.重点企业遴选。以粗钢产量为基准，综合技术装备先进程度、年营业收入等因素，在粗钢年产量超过 1000 万吨的大型钢铁集团等企业中遴选重点企业。

2.重点场景保护。围绕铁前、炼铁、炼钢、轧制等业务

场景，重点提升冶炼控制参数、国家重大工程或重点型号用特殊钢领先工艺、大宗原材料信息等数据在收集、传输、使用和加工环节中的安全保护能力。

3.安全防护强化。推动核心生产设备软硬件自主可控，防范关键技术参数泄露、篡改和远程窃取等风险。针对钢铁行业工业互联网平台，强化入侵防范、访问控制、重要数据加密存储等能力。

4.标准规范研制。加快钢铁行业数据安全标准研制，统一数据分类分级标准，加大标准在行业内的应用推广力度。

5.典型应用推广与人才培养。培育一批行业内应用成效好、具备可复制可推广条件的数据安全解决方案，加强典型实践案例宣传推广。强化钢铁行业数据安全管理人员培训，加快行业数据安全专业人才培养。

二、有色行业

（一）工作目标

到 2026 年底，有色行业开展数据分类分级保护的规上工业企业超 500 家，行业数据安全保护意识普遍增强；立项研制行业数据安全标准规范 5 项；推动 50 家以上企业建设数据安全技术手段，指导提升风险防范和处置能力；遴选行业数据安全典型解决方案 10 个，形成可复制可推广的行业实践模式。

（二）重点任务

1.重点企业遴选。将中国有色金属工业协会每年发布的

有色金属企业营业收入 50 强企业，以及稀土、稀有金属主要企业等作为重点企业。

2.重点场景保护。围绕采矿与矿石处理、有色金属冶炼、材料制备加工、物流与运输、销售与供应链等业务场景，关注矿产资源信息、原辅料及产品库存量、采购量、销量、生产计划、供销渠道、关键工艺过程、敏感经济指标等数据在收集、传输、存储、交换、出境等环节的数据安全防护与风险防范。制定安全防护实操指引，指导企业强化数据安全风险评估等能力。对于向数据存储在海外的信息系统填报数据以及非政府组织、境外司法调取数据，严格落实数据出境安全评估、主管部门审核报批等要求。

3.标准规范研制。加快推动有色行业数据分类分级、重要数据识别、数据安全防护、风险评估等标准制定，加大标准在行业内的应用推广力度。

4.典型应用推广。组织遴选在行业内应用成效好、具备可复制可推广条件的数据安全解决方案，加强典型实践案例宣传推广，打造一批行业数据安全标杆企业。

三、石化化工行业

（一）工作目标

到 2026 年底，石化化工行业开展数据分类分级保护的规上工业企业超 100 家，立项研制数据安全标准规范 5 项，分类分级、应用数据安全等关键标准供给能力显著增强；形成石化化工行业数据安全风险事件及数据安全典型解决方

案案例集。

（二）重点任务

1.重点企业遴选。将中国石油和化学工业联合会、中国化工企业管理协会联合发布的中国石油和化工企业 500 强企业等作为重点企业。

2.重点场景保护。围绕原油加工、炼化、基础化学原料制造、煤炭加工、肥料制造、精细加工、化工园区等业务场景，加强对生产数据、工艺参数、能耗数据、科研创新数据、供应链管理数据等重要数据加密和备份，强化数据全生命周期安全保护。针对生产控制系统、生产运营系统、物联网平台、供应链管理平台等重点系统平台，建立数据安全监测与保护能力，实现数据安全汇聚与交换共享。加强对特种工程塑料、高性能膜材料、电子化学品等行业关键材料的全过程数据的脱敏和备份。聚焦勒索病毒攻击、供应链攻击、网络攻击等风险易发或高发场景，加强数据安全风险监测预警与排查防范。

3.标准规范研制。结合石化化工行业智能制造标准体系建设指南，鼓励行业协会、科研院所、企事业单位、高等院校等共同推动石化化工行业数据安全标准制定。

4.典型案例编制。培育一批行业内应用成效好、具备可复制可推广条件的数据安全解决方案。梳理石化化工行业勒索病毒攻击、数据泄露等数据安全风险事件及应急处置方案，组织编制石化化工行业风险事件案例集，加强警示宣传。

5.人才队伍建设。注重行业企业数据安全管理工作、建设实施、应急处置等能力，充分发挥高等院校、科研院所及数据安全专家作用，打造数据安全人才队伍，加强行业从业人员交流沟通，基本完成石化化工行业数据安全“教、学、研、管、评”体系建设。

四、汽车行业

（一）工作目标

到 2026 年底，汽车行业开展数据分类分级保护的规上整车企业超 50 家，数据安全宣贯培训覆盖 3000 人次，数据安全保护意识普遍提高；立项研制数据安全标准规范不少于 20 项，分类分级、出境安全、个人信息保护、应用数据安全等关键标准供给能力显著增强；组织开展专项行动，加强数据安全风险排查与防范；遴选不少于 10 个数据安全典型案例，形成可复制推广的数据安全实践经验。

（二）重点任务

1.重点企业遴选。整车企业覆盖国内自主品牌企业、合资企业和外资企业，将年产量大于 10000 辆的商用车企业、年产量大于 50000 辆的乘用车企业等作为重点企业。

2.重点场景保护。面向汽车研发、生产等业务场景，体系化建立数据安全保护能力。针对车联网服务平台及联网系统，强化大规模数据细粒度访问控制、数据加密、数据脱敏共享等能力，加强数据安全风险监测预警与排查防范和数据全生命周期安全保护。聚焦勒索病毒攻击、云平台攻击等风

险易发或高发场景，加强数据安全风险监测预警与排查防范。

3.标准规范研制。持续完善汽车数据安全标准体系顶层设计，鼓励科研院所、企事业单位、高等院校、行业学会、协会、联盟团体等各类主体积极参与汽车行业重要数据识别准则、数据脱敏、供应链安全管理要求、数据安全检测评估及服务能力要求等标准制定。

4.关键技术研究。推动汽车行业数据加密、数据脱敏、数据溯源、隐私计算、数据安全测试工具、数据安全监测平台等关键技术研发创新。强化数据安全监测预警和应急处置技术，提高对终端、网络、云平台等场景中数据流动和异常行为监测的准确性，提升风险事件处置自动化、智能化水平。

5.服务能力提升。建立汽车行业数据安全服务能力，支持开展汽车行业数据安全产品、服务及体系认证。

6.人才队伍培养。组织开展汽车行业数据安全能力提升培训，支持汽车行业数据安全从业人员资格认定，加快培养汽车行业复合型数据安全人才。

五、民机行业

（一）工作目标

到2026年底，民机行业开展数据分类分级保护的规上工业企业超5家，数据安全宣贯培训覆盖2000人次，数据安全保护意识普遍提高；开展数据安全标准规范研制；遴选

数据安全典型案例，形成可复制推广的数据安全实践经验。

（二）重点任务

1.重点企业遴选。围绕飞机研发设计、生产制造、试验试飞、市场营销等全生命周期业务环节，根据承接业务量、技术实力、主导地位等指标，依照排名情况遴选骨干企业作为重点企业。

2.重点环节保护。加强机体供应商、适航当局及客户信息等数据在使用环节中的访问控制和权限管理。部署数据库审计、备份等防护措施，保障企业重要数据和敏感数据的存储安全。

3.重点场景保护。围绕机载航电、试验试飞、运行支持等典型场景，聚焦数据中台、机载设备、制造设备、试验设备等关键设备平台，加强数据安全技术研究、风险分析、漏洞验证与修复，防范数据大规模泄露、批量窃取、恶意篡改等风险。

4.标准规范研制。组织开展民机行业数据安全标准建设，研制民机细分行业的数据分类分级、重要数据识别等标准规范。

5.关键技术研究。结合民机行业的实际特点，加大安全类产品自主可控研发利用的资源保障，形成民机行业特有的数据安全组件和工具。

6.人才队伍培养。组织搭建网络与数据安全综合培训体系。培养一批具有民机制造业背景的数据安全攻防技术研究

的专业“蓝军”，提升民机行业高等级威胁攻防对抗能力。

六、民船行业

（一）工作目标

到 2026 年底，民船行业开展数据分类分级保护的规上工业企业超 20 家，数据安全宣贯培训覆盖 2000 人次，数据安全保护意识普遍提高；立项研制数据安全标准规范 10 项，数据加密、备份恢复等关键标准供给能力显著增强；遴选不少于 5 个数据安全典型案例，推动对现有制造和营运船舶的数据安全改造升级。

（二）重点任务

1.重点企业遴选。将年度船舶企业手持订单量及完工量排名前 10 的民船企业等作为重点企业。

2.重点环节保护。重点关注航行监控和导航、维修和故障诊断、货物和舱位管理、安全风险管理等数据的使用加工环节，配备数据安全审计、权限管理、数据脱敏等防护手段。加强船舶通信数据、航行计划数据等在传输环节的风险监测。针对船舶研发设计信息、生产状态监测信息、船舶导航和船岸通信等重要数据的存储环节，加强身份认证与数据加密。

3.重点场景保护。面向船舶性能模拟与优化、船舶系统集成与布局设计、船体制造与焊接、船舶运行监控与调度等典型场景，加快提升数据安全保护能力。针对船舶导航系统、船舶通信系统、岸端系统，加强“船内-船舶-船岸”通信边

界安全与数据传输安全应用研究，完善安全策略和规则。开展数据安全风险评估、监测预警与排查，防范船舶装备后门漏洞、勒索攻击、上云等风险。

4.标准规范研制。开展船舶数据安全标准规范制修订工作，规范相关术语，推动数据分类分级、数据传输与交换等标准建设。积极参与和促进国际海事公约数据安全相关标准规范的制修订。结合国际国内船舶数据安全防护体系的发展，不断完善船舶数据安全防护规范及相关检验指南。

5.关键技术研究。开展基于国产密码技术的船舶办公自动化、视频监控、安全组网、访问控制、船岸通信等业务场景的数据加密保护研究，形成船舶行业特有的数据安全设备。推动同态加密、安全多方计算等技术在数据密态流通方面的创新突破，实现多源异构数据安全融合，提升船舶数据共享保障能力。强化船舶重要数据备份恢复技术能力，执行合理备份策略，推动建设容灾中心，降低数据恶意篡改、非法获取等风险。

6.推动试点应用。积极推进船舶数据安全防护应用，选择商船、渔船、客船等不同类型和规模的船舶为试点对象，以新建安全船舶的试点，带动营运船舶的数据安全防护升级，不断扩展各类船舶设备数据安全防护应用范围。

7.人才培养。组织开展船舶行业数据安全能力提升培训，加快培养船舶行业复合型数据安全人才。

七、纺织行业

（一）工作目标

到 2026 年底，面向纺织行业规上企业推动开展数据分类分级保护；数据安全宣贯培训覆盖 2000 人次，数据安全保护意识普遍提高；纺织行业工业互联网平台数据安全防护制度基本完善；开展分类分级等数据安全标准规范研制；遴选不少于 20 个数据安全典型案例，形成可复制推广的数据安全实践经验。

（二）重点任务

1.重点企业遴选。将世界 500 强企业、中国制造业 500 强企业中的纺织企业等作为重点企业。

2.重点环节保护。加快提升化纤、纺纱、织造、印染、服装、产业用纺织品等细分行业的生产数据、工艺数据、客户数据的安全保护能力，加强高新技术纤维的研发和生产等重要数据的全生命周期安全管理与防护。加强产业链供应链数据出境安全评估。

3.重点场景保护。针对纺织行业工业互联网平台，强化大规模数据细粒度访问控制、重要数据脱敏共享等能力，实现数据安全汇聚与交换共享。聚焦内部人员操作不规范、勒索病毒攻击、技术服务外包、重要数据暴露等风险易发或高发场景，加强数据安全风险监测预警、排查与防范。

4.标准规范研制。推动建立纺织行业数据安全标准体系，研制数据安全标准规范，在典型企业组织开展标准验证、应用工作。

5.应用案例推广。培育一批行业内应用成效好、具备可

复制可推广条件的数据安全解决方案，遴选数据安全典型案例，并在全行业内宣传推广。

八、集成电路行业

（一）工作目标

到 2026 年底，集成电路行业开展数据分类分级保护的规上工业企业超 50 家，数据安全宣贯培训覆盖 1000 人次，数据安全保护意识普遍提高；开展分类分级数据安全标准规范研制；遴选不少于 10 个数据安全典型案例，形成可复制推广的数据安全实践经验。

（二）重点任务

1.重点企业遴选。围绕集成电路设计、代工制造、封装测试、半导体材料及设备等产业环节，依据年度总销售收入及细分领域市场占有率等遴选重点企业。

2.重点环节保护。加强材料配方、熔炼工艺、零部件核心技术指标、刻蚀设备等运行参数、EDA 仿真算法等数据安全管理与防护，关注对外提供等环节中的供应商遴选与资质审核。对于境外司法调取数据，严格落实数据出境安全评估、主管部门审核报批等要求。

3.重点场景保护。面向集成电路设计、制造、封装测试等业务场景，加强企业 IP 使用审核、光罩运输追踪、报废晶圆保护、封装测试等应用场景的数据安全防护和管理，重点防范勒索攻击、员工不当操作等风险。

4.标准规范研制。推动集成电路行业数据安全标准规范

建设，加快制定数据分类分级、重要数据和核心数据识别、安全风险监测、数据出境安全评估、数据安全产品分类评价等细化标准。

5.服务能力提升。联合数据安全相关研究机构，完善数据安全监测、预警、溯源等技术能力，提供数据安全风险监测、溯源与数据安全检测、认证、评估等咨询服务。

6.建立行业激励机制。将数据安全纳入重大集成电路项目的考核指标评价体系，鼓励数据安全产品和服务在集成电路行业中推广应用。

7.人才队伍培养。系统组织开展集成电路行业数据安全教育和培训，加快培养集成电路行业复合型数据安全人才。

九、软件行业

（一）工作目标

到 2026 年底，软件行业开展数据分类分级保护的企业超 200 家，数据安全宣贯培训覆盖 3000 人次，数据安全保护意识普遍提高；遴选不少于 10 个数据安全典型案例，形成可复制推广的数据安全实践经验。

（二）重点任务

1.重点企业遴选。围绕国家鼓励的重点软件企业、专精特新中小企业、行业龙头企业等遴选重点企业，覆盖基础软件、工业软件、行业应用软件、新兴平台软件、嵌入式软件等软件行业各重点方向。

2.重点场景保护。围绕软件研发设计、开发部署、运行

维护等业务环节，完善数据安全分区、分级防护要求。强化软件算法、源代码等数据的安全防护，加强开源代码合规管理与安全防护。完善国内开源代码托管平台安全机制，提升应对勒索攻击、数据篡改等安全风险的技术能力。加强远程运维、软件云化服务、人工智能模型开发训练等新兴场景的数据安全监管，防范大规模数据泄露与窃取风险。强化软件与硬件、网络等数据安全能力协同部署，提升安全防范水平。

3.安全风险防范。强化软件产品源代码数据安全漏洞审查和保护。组织开展软件开源组件安全风险评估检测，推动实施“开源项目白名单”。加强产品 API 安全防护，及时检测 API 在认证、授权、数据暴露、输入检查、安全配置等方面的安全漏洞。完善软件产品安全漏洞专业库建设，重点防范因漏洞、后门不受控造成的数据丢失、供应链安全等风险。

4.典型应用推广。围绕软件行业数据安全风险特性，加快重点领域技术产品研发创新，加强典型实践方案宣传推广，打造一批行业数据安全解决方案。

5.保护意识提升。面向软件行业加强数据安全法律法规和政策标准的宣贯培训，督促指导软件厂商增强数据安全保护意识和能力。

6.人才培养。依托特色化示范性软件学院等，系统组织开展软件行业数据安全教育和培训，加快培养软件行业复合型数据安全人才。

信息公开属性：主动公开

抄送部内：相关司局。

工业和信息化部办公厅

2024年2月27日印发

