智能体规范应用与创新发展实施意见

智能体是具备自主感知、记忆、决策、交互与执行能力的智能系统，是人工智能产品及服务的重要形态。随着大模型等新一代人工智能技术迅猛发展，智能体正加速与网络空间、物理世界深度融合，深刻改变人类生产生活方式和社会治理模式。为落实国务院《关于深入实施“人工智能+”行动的意见》，促进智能体规范应用与创新发展，制定本实施意见。

一、基本原则

以推动科技创新、提升治理能力、构建产业生态、增进民生福祉为导向，坚持安全可控，将智能体安全、可靠、可信作为发展的底线要求，贯穿智能体技术研发、应用部署与推广的全过程，切实防范系统性风险。坚持规范有序，适应智能体技术演进规律，构建与现有政策法规衔接顺畅、行业自律自治、底线红线清晰的治理体系，有序推进智能体落地应用。坚持创新驱动，加强理论创新、技术创新、工程创新联动，体系化突破智能体关键技术，完善政产学研用协同机制，构建开放共享的智能体生态，提升产业创新活力。坚持应用牵引，重点围绕科学研究、产业发展、提振消费、民生福祉、社会治理等实际需求，发挥典型应用场景示范效应，先易后难、循序渐进，促进智能体技术验证、产品迭代、应用落地。

二、夯实发展基础

夯实技术底座，健全标准体系，降低智能体研发、适配、应用门槛，为丰富智能体产品及服务奠定基础。

（一）完善技术底座

1.强化基础技术研发。持续提升通用基础模型性能，支持行业发展细分领域专用模型，形成适应不同场景和设备的模型产品矩阵。面向智能体训练与运行，提升高质量数据集供给能力。加强智能体任务理解、任务规划、工具使用、长期记忆、互认互通、群体协同等技术攻关，提升智能体泛化能力。

2.完善智能体工具链。开展智能体底层框架研究，加快研发感知、记忆、决策、交互、执行等关键组件，完善智能体研发、测试、部署、运维等工具链。发展对抗样本检测、行为异常检测等安全与治理工具，提升对智能体非合规行为的发现、干预、阻断、恢复能力。

（二）构建标准协议

3.建立智能体标准体系。制定智能体标准化工作指导文件，形成智能体标准框架，系统布局关键技术、重要产品、数据交换、应用场景、质量评测、安全保障、可信认证等标准体系，加快制定智能体与软件工具、应用服务、硬件外设接口等基础标准。加强智能体互联协议（AIP）等智能体互联关键国家标准、行业标准的推广应用。支持医疗、交通、媒体、公共安全等领域制定强制性标准。鼓励企业按照相关标准研发产品服务，提升智能体规范性。积极参与国际标准制定。

4.布局发展智能互联网。研究建立智能互联网体系架构，探索建立智能体注册平台，提供智能体数字身份管理、检索发现、能力声明等服务，支持开发者、部署方式、接口协议、合规认证等信息查询和管理。提升多智能体协同能力，研究智能体身份标识、可信互联、合规支付、安全防护、冲突解决等基础技术。发挥互联网协议第六版（IPv6）技术优势，提升智能体端到端通信能力。探索建立智能互联网监测指标体系。

三、守牢安全底线

坚持以人为本、智能向善、多元共治、安全稳妥，营造规范发展、鼓励创新的制度环境，促进智能体健康有序发展。

（一）明确产品准则

5.完善政策法规和伦理规范。加快研究智能体相关政策法规及伦理规范，发挥专业机构内容资源和审核把关优势，确保智能体行为符合法律法规及主流价值观。防止智能体利用数据优势、人格化技术实施传播不良价值观、算法压榨等行为，防范未成年人、老年人沉迷成瘾、情感依赖等风险。做好与人工智能伦理审查等制度衔接。

6.明确决策权限。在遵守法律法规、尊重社会公德和伦理规范前提下，厘清仅限用户本人决策、需由用户授权决策和智能体自主决策等各种决策方式的合理边界及所需权限。确保用户对智能体自主决策享有知情权和最终决策权，智能体执行操作不得超出用户授权范围。

7.加强行为管控。发展规则内嵌、行为围栏等技术，确保智能体在公共场所、隐私场所、专门场所等的行为合法合规。探索利用区块链等技术，建立重要应用场景智能体行为可验证、可追溯机制，防范智能体不当行为引发重大风险。

（二）防范安全风险

8.提升内生安全能力。研究智能体数据安全、个人信息保护、密码防护、攻击检测、权限管理、行为控制等安全技术，提升智能体系统安全保障能力，防范数据投毒、隐私泄露、算法篡改、系统漏洞、运行失控等安全风险。研究智能体安全检测技术，探索建立智能体安全评估体系。

9.加强供应链安全。制定智能体开发、部署、应用、维护等全周期安全规范，加强模型接入、应用程序接口调用、扩展工具使用等环节安全管理。探索建立智能体供应链安全信息共享和预警机制，及时发布风险提示，提升安全保障能力。

10.化解应用衍生风险。完善智能体常态化风险识别、预警及干预机制，强化人机协同审核、拦截阻断等风险处置能力，防范系统性安全风险。强化智能体应用安全管理，避免智能体被用于自动化攻击、隐私侵犯、虚假信息生成传播、网络诈骗等违法犯罪行为。

（三）完善治理体系

11.构建分类分级治理框架。根据应用场景和潜在影响，审慎稳妥开展智能体分级治理。对于敏感领域及重点行业，由网信部门联合行业主管部门确定开放场景，根据相关法律法规、监管要求和安全防护标准，实行备案、检测、问题产品召回等管理措施。对于部分生活娱乐、日常办公等低风险领域，完善智能体评估测试工具，通过合规自测、信息报告、分发平台管理、行业自律等实现高效治理。

12.健全合规服务体系。强化智能体风险监测预警、检测评估、咨询、认证等专业服务供给，引导行业积极研发智能体监测工具。开展智能体功能、性能、质量、合规等第三方评测服务，推动认证与检测结果互通互认，为用户选择智能体提供参考。编制并发布智能体技术及应用成熟度报告，为产业研发应用提供参考。

（四）强化行业自律

13.引导行业加强自律。鼓励行业组织、主要企业联合制定行业自律规则，明确智能体功能合规、算法治理、知识产权保护、公平竞争等规范细则。指导智能体开发平台、分发平台、服务提供者建立公平合理的平台规则、用户服务协议及隐私政策，明确供需双方权责，保障产业健康发展。加强智能体应用风险宣传教育，提升用户安全意识。

14.探索信用评价机制。指导行业组织建立智能体市场主体自愿参与的信用评价机制，对于技术滥用、诱导消费、虚假宣传、隐瞒缺陷信息等行为进行信用评价，依法依规开展失信惩戒。引导智能体开发者、开发平台、分发平台、服务提供者等参与信用评价，共同营造良好发展环境。

四、强化应用牵引

积极稳妥推动智能体典型场景应用，牵引技术产品优化提升，探索形成可复制、可推广的智能体落地应用模式。

（一）科学研究

15.科研探索。研发理论推演、模拟仿真等智能体，挖掘潜在技术路径。强化智能体信息关联整合、知识体系构建等能力，提升自然科学、哲学社会科学研究发现能力。促进智能体与科学仪器、实验平台融合，实现方案设计、实验操作、数据处理、结果分析等全流程智能化。

16.研发辅助。发展软件开发智能体，提升需求分析、架构设计、代码生成与测试等全流程开发能力。促进智能体与计算机辅助设计（CAD）、计算机辅助工程（CAE）等软件结合，提供设计方案生成、仿真验证、参数调优等功能。

（二）产业发展

17.智能制造。研发生产管理智能体，动态优化生产排程、资源分配和工序衔接，推动智能体在工业互联网领域应用，提升企业精细化管理水平。提升智能体工艺参数优化、加工精度检测、产品缺陷识别等能力，促进智能体与数控机床、工业机器人、自动化产线等融合，促进提质增效降本。

18.能源资源。研发大气、水体、土壤、噪声等环境要素感知智能体，提升自然灾害、环境污染等风险预警能力。依托智能体强化对国土空间资源全周期管理能力。依托智能体实现能源、金属等矿产资源高效勘探。发展电力调度、用电监测、电网维护等智能体，提升电力资源使用效率。

19.交通运输。研发交通安全监管、应急指挥调度等智能体，提升违章违规行为识别、交通基础设施风险预警、重点车辆（船舶）监管、事故快速响应等能力。优化交通监测调度智能体性能，发展交通载运工具管控智能体，提升路网、水网、空域的通行效率。

20.农业生产。研发农业服务智能体，开展农技指导、病虫害诊断与防治等服务。推动智能体在种植养殖、高效育种等环节应用，推进农业智能化转型。推动智能体与智能农机具、智慧大棚、农业服务平台融合，提升农业生产效率。

21.金融服务。研发金融风控智能体，提升信贷审批、交易监控、账户安全等环节风险识别能力。完善智能体异常检测、合规审计功能，提升信贷违约预测、信用卡盗刷拦截、反洗钱监测等能力。

（三）提振消费

22.终端应用。推动智能体赋能互联网应用及服务，优化在线购物、出行导航、生活缴费、日常办公等服务体验。推动智能体与手机、电脑、汽车、家居、可穿戴、消费级机器人等终端设备协同发展，提升跨应用、跨设备任务完成能力。

23.文化旅游。研发文学、音乐、绘画、视听、演艺等内容创作智能体，促进优秀文化传播推广。发展智能导览、多语种翻译、适老适残等旅游服务智能体，提升旅游服务水平。

24.商业服务。提升智能体客服能力，提供7×24小时咨询、预约、售后等服务。发展导引、清洁、仓储、配售等具身智能体，提升餐饮、零售、住宿、物流等商业场所的运营效率。探索通过具身智能体提供低成本家政、养老、托育、助残等服务。

（四）民生福祉

25.教育教学。探索课件生成、作业批改、学情分析等智能体，提高教师工作效率。依托智能体开展个性化学习方案制定，完善智能导学、答疑辅导、虚拟助教等功能。支持在线教育平台研发智能体，提供终身学习服务。

26.医疗健康。提升医学影像分析、疾病诊断推理、定制化诊疗方案生成等医疗辅助智能体性能，探索药品管理、手术排程、病历管理等智能体，提升医疗服务效率。稳步发展预问诊、报告解析等智能体，提升患者体验。

27.人力资源。探索智能体在就业促进、技术技能人才培养评价、劳动关系公共服务等领域应用，提升就业服务能力。发展社会保险、劳动争议仲裁、欠薪治理等智能体，保障劳动者合法权益。

28.信息服务。探索智能体在网络内容建设管理中的应用，鼓励信息发布部门和内容传播平台研发用户分析、选题策划、采编加工、分发推荐、智能审核、舆论引导、情绪疏导、实时翻译等智能体，实现多模态信息、跨领域信息的高效整合。

（五）社会治理

29.政务服务。探索事项辅助审批智能体，推动政务审批流程智能化。发展政策咨询智能体，提供全天在线的政务咨询、流程指引等服务。探索主动推送适配政策、服务提醒及办理指南，加快从“人找服务”向“服务找人”转型。

30.司法服务。探索全流程办案辅助智能体，提升案件材料梳理、案件信息录入、证据审查、辅助法律文书生成等能力。发展法律宣传、法律咨询、法律监督等智能体，为群众提供高效便捷的在线司法服务。

31.公共安全。探索监测预警、应急处置、救援调度、协同治理等智能体，提升安全生产监管和防灾减灾救灾等能力。提升智能体异常行为识别、潜在威胁预警、动态防控处理能力，维护公共安全。推动具身智能体在灾害救援、安防巡检、危险品处置等领域落地应用。

32.城市治理。探索智能体在城市规划、建设与治理环节应用，支撑智能建造、房屋管理、城市基础设施安全运行等工作，提升城市治理专业化水平，提升城市人居环境质量。

33.招标投标。探索招标投标智能体，实现招标投标活动全链路智慧管理，保障全过程规范高效。提升招标投标交易、服务和监管的智慧化水平，实现招标科学合理、评标公平公正和监管穿透高效。

五、建设创新生态

畅通供需渠道，促进研发侧、需求侧高水平互动，形成市场牵引、内驱发展的智能体产业生态。

（一）促进产业合作

34.培育开源创新力量。引导国内人工智能开源社区加强智能体布局，开展智能体与开源芯片、开源操作系统、开源大模型兼容适配。引导企业、高校、科研机构积极参与智能体框架、交互接口、工具链等开源项目，推动技术体系融通发展，加快提升国际影响力。

35.搭建产业协作平台。发挥智能体相关生态联盟、技术验证实验室等产业协作平台的作用，协同产业链上下游开展智能体共性技术研发、标准制定、评估认证等工作，开展智能体技术与产业应用复合人才培养。引导互联网应用、智能终端等领域企业共建生态，探索建立互利共赢的合作模式。

（二）强化应用推广

36.构建应用推广渠道。推动建立智能体软件商店、行业供需信息发布平台，引导智能体企业积极发布产品，形成集聚效应。开展智能体应用供需对接活动，采取公开招标、揭榜挂帅等方式吸引智能体企业定制化开发相应产品。引导整机、软件等企业基于智能体研发产品和服务，培育用户市场。

37.推进重点场景开放。推动重点领域开放智能体应用场景，在产业集聚区、重点行业、重点领域开展智能体应用试点，打造一批具有引领作用的示范项目。发展市场化、专业化的智能体技术转化服务机构，探索智能体应用场景，提升技术成果转化效率。促进行业数据共享开放，支撑重点场景智能体训练部署。

38.积极培育全球生态。依托世界人工智能大会、世界互联网大会等国际平台，交流展示智能体技术创新成果。推动终端设备、软件企业适配智能体，引导相关企业做好海外合规建设，推动智能体适应当地法律法规和文化习俗。

六、保障措施

国家网信办、国家发展改革委、工业和信息化部会同有关方面加强统筹谋划，强化资源整合和力量协同，完善配套政策，形成工作合力，推动重点任务落实落地。建立并完善智能体发展评价指标体系，加强智能体规范应用与创新发展的监测评估、滚动实施和动态调整。