

云上智能体服务网络和数据安全自律公约

（2026 版）

第一章 总则

第一条 为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全条例》《工业和信息化领域数据安全管理办法（试行）》等法律法规和政策要求，推动云上智能体服务安全健康发展，实现人工智能技术创新应用高质量发展和高水平安全良性互动，制定本公约。

第二条 本公约所称云上智能体是指在云环境上部署运行，以大模型为决策与编排核心，通过技能、工具访问用户数据与系统，具备一定自主规划与任务执行能力，并能在多种入口（网页、客户端、即时通讯工具、应用平台等）接收指令并代表用户采取行动的智能系统。

第三条 本公约旨在规范提供云上智能体服务的云服务商，防范智能体在安装前、部署时、运行使用过程中各环节的网络和数据安全风险，维护用户使用智能体的安全与合法权益。本公约适用于云服务商提供预装 OpenClaw 等智能体服务的情形。

第二章 自律条款

第四条 与用户签订云服务协议，根据业务模式和服务内容，明确双方的安全责任义务。

第五条 向用户提供从智能体官方渠道下载的最新稳定版本，安装前完成镜像程序及运行环境必要的安全检测和防护，安装时通过虚拟机或容器等方式做好服务运行环境隔离，关闭互联网访问端口，设置智能体的独立工作文件目录，开启自动更新提醒。根据用户需要，提供云平台安全网关中转、网络安全隧道等远程访问服务。

第六条 做好云平台数据传输、存储的基础性数据安全保障。根据用户需要，向用户提供密钥管理和数据加密服务，支持用户实现 API Key 等敏感数据安全存储，以及智能体云环境工作文件目录数据加密的能力，提供配置文件、长期记忆文件等敏感数据外发的安全监测阻断能力，协助用户有效防范数据窃取风险。

第七条 根据用户需要，提供以下服务：定期排查智能体互联网访问端口，一旦发现及时提醒用户关闭；提供恶意技能和插件的安装前安全检测、运行时安全监测、定期安全扫描、行为安全审计等服务；提供智能体交互数据的安全检测识别、拦截处置等服务，防范提示词注入攻击、有害指令、高危风险行为等安全风险。

第八条 加强用户安全宣传，积极向用户提供含智能体身份权限设置、智能体互联网访问控制、文件系统访问控制等智能体部署的安全配置模板或实践指南。通过用户界面、产品说明等形式，向用户明确告知智能体服务潜在的网络和数据安全风险。根据用户需要，提供网络和数据安全产品或服务供用户选择，助力用户提升安全防护能力。

第九条 及时向电信主管部门报送云上智能体的风险信息、实践案例、安全事件及处置方案等信息，协同应对重大安全风险。

第三章 公约的执行

第十条 中国通信学会网络和数据安全专业委员会协同中国人工智能产业发展联盟安全治理委员会作为本公约的执行机构，负责组织实施本公约。

第十一条 云上智能体服务云服务商签署本公约后受本公约约束，遵守执行本公约内容。

第四章 附则

第十二条 本公约经公约签署单位加盖单位公章后生效，自公布之日起施行。