

《安全可信AI云电脑能力要求》 标准编制说明

标准起草组

2025 年 05 月 13 日

1、 标准范围。

本规范旨在定义安全可信AI云电脑能力要求，帮助企业明确安全可信 AI 云电脑的整体框架、关键能力指标，从安全可信、产品质量双维度规范产品能力，并给出能力评价的成熟度模型。

随着人工智能与云计算技术的深度融合，AI 云电脑作为创新产品，已在办公、教育、娱乐等多领域广泛应用，极大提升了资源利用效率与用户体验。基于自主基础软硬件构建的安全可信AI云电脑以数据高度安全、系统高度可控、适配性强且兼容性佳、有效抵御外部攻击等优势成为党政、医疗等行业首选智能解决方案，对推动行业数字化转型具有重大意义。

2、 工作简况。

本项目计划名称为“安全可信AI云电脑能力要求”。由中国互联网协会归口。由中国信息通信研究院牵头研制。

本文件起草单位包括中国信息通信研究院、阿里云计算有限公司、中移（苏州）软件技术有限公司、联通数字科技有限公司、天翼云科技有限公司、中移（杭州）信息技术有限公司、四川虹微技术有限公司；

本文件主要起草人：

本文件于2025年5月在中国互联网协会通过立项申请。

起草组于2025年6月召开线上讨论会，汇报讨论标准的研制情况。会上各企业根据产品的共同需求及差异性进行讨论，对标准中的相关内容提出合理建议，最终形成符合在线文档行业要求的标准文件。

3、 标准编制原则和确定标准主要内容的依据：

编制原则：

- 标准性要求，充分借鉴国内相关标准规范，并结合我国实际情况，力求该标准的可执行性和规范性更强；
- 实用性要求，依据法律法规和行业需求特性，明确技术要求与可信验证机制，厘定产品功能边界，构建基础环境适配、软硬件设施、平台功能的全链条统一标准，规范产品研发、部署应用、服务保障等全生命周期活动。具有充分的技术先进性和实用性
- 可行性要求，结合当前主流技术栈和企业技术储备现状，制定分层级、可落地的技术要求。
- 有效性要求，考虑到技术的发展与扩充需求，故全面考虑标准架构和兼容性，满足未来标准发展与扩充需求。

4、 主要试验（或验证）的分析、综述报告。

本标准的技术内容聚焦安全可信AI云电脑平台的全维度能力构建，经过对各方场景业务及技术方案的调研与分析，通过对各参与方不同产品在技术与需求方面的讨论，得到了符合行业要求的通用技术文档，最终形成的标准文件得到各参与方的认可和验证，标准可为从事安全可信 AI 云电脑研发、应用及评价的各类机构提供参考。

5、 标准在起草过程中遇到的问题及解决办法：重大分歧意见的处

理经过和依据：有无重要技术问题需要说明。

在标准起草过程中遇到的问题通过项目组内部协调和讨论已经解决。无重大分歧意见。没有重要技术问题需要说明。

- 6、 与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

本标准无对应的国际标准或国外标准。

- 7、 修订标准时，说明与标准前一版本的重大技术变化，并列岀所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/代替现行有关标准的建议：

本标准为第一版制定标准。

- 8、 说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

本标准与其他标准或文件无关系。

- 9、 标准作为强制性标准或推荐性标准的建议：

建议本文件作为推荐性团体标准发布实施。

- 10、 贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

本标准的发布与实施可协调产业共识，促进行业健康发展，形成产品统一要求和考量，从而为该类产品的未来能力发展和普及奠定技术保障。

- 11、 标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

本文件不涉及知识产权的问题。

- 12、 其他应予说明的事项。

无。