

《智能AI安全控制系统技术规范》
(征求意见稿)

编制说明

《标准名称》 编制组

二〇二五年1月

《智能 AI 安全控制系统技术规范》（意见征求稿）

团体标准编制说明

一、工作简况

（一）任务来源

本标准由中网华信科技股份有限公司提出,中国联合国采购促进会归口。本文件规定了智能 AI 安全控制系统的技术规范,本文件编制的目的是应对 AI 技术在快速发展和应用过程中所带来的安全与合规性问题。

（二）起草单位情况

本标准起草单位包括：中网华信科技股份有限公司。

（三）标准编制过程

（1）成立标准起草组，技术调研和资料收集

2024 年 11 月 05 日—11 月 15 日，为保证制订工作的顺利开展、提高标准的质量和可用性，由起草单位和相关技术专家共同组建了标准起草组，负责对智能 AI 安全控制系统技术规范标准编制进行确定。通过制订工作方案，标准起草组进一步明确了目标要求、工作思路、人员分工和工作进度等。

标准起草组对相关指标和要求进行了调研，搜集了众多 AI 技术相关的标准、文献、成果案例等资料，着手标准制定。

（2）确定标准框架，形成标准草案

2024 年 11 月 16 日—11 月 24 日，起草小组结合前期的调研和资料，多次召开内部研讨会，形成标准大纲，并邀请了专家和相关企业对标准进行技术指导，对《智能 AI 安全控制系统技术规范》的标准编制工作重点、标准制定依据和编制原则等形成了共识，同时完成标准草案稿的撰写。

二、标准制定的目的和意义

（1）目的：立项《智能 AI 安全控制系统技术规范》标准的主要目的该标准的制定旨在解决 AI 技术在其迅猛进步及广泛应用背景下所产生的安全与合规挑战。鉴于 AI 技术已深入渗透至多个行业领域，伴随而来的安全隐患也日渐显著，具体表现为数据隐私保护缺失、算法决策中的偏见问题、以及模型运作缺乏透明度等。为此，我们亟需构建一套全面的技术规范框架，以保障 AI 技术在稳定且受控的条件下发展，从而有效缩减潜在的安全风险至最低限度。

（2）意义：提升 AI 技术的安全性和可靠性：通过制定严格的技术规范，可以确保 AI 系统在数据采集、算法开发、产品测试及市场推广等全生命周期中，都遵循相应的安全标准和伦理要求。这有助于提升 AI 技术的整体安全性和可靠性，保障用户的安全和权益。

推动 AI 行业的规范化和智能化发展：标准的实施将为企业明确的操作指引，促进 AI 行业的规范化和智能化发展。同时，这也有助于提升公众对 AI 技术的信任度，推动 AI 技术在更广泛的领域中得到应用。

加强国际间的交流与合作：鉴于全球对 AI 监管的日益关注，各国政府正积极制定法规以规范 AI 技术的发展。在此背景下，立项《智能 AI 安全控制系统技术规范》标准，能够增进国际间的信息共享与合作，携手促进全球技术安全与伦理责任的落实。

促进经济社会的转型与进步：AI 技术作为当前科技革命与产业变革的引领者，已成为国家经济与社会发展的核心动力。通过制定并实施相应的技术规范，能够引导企业在技术创新中更加关注用户需求，优化产品体验。这一举措将有力推动经济社会的转型升级，助力实现高质量发展目标。

三、标准编制依据

本标准在编制的过程中遵循“先进性、科学性、可操作性”的原则，按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

四、标准主要内容

本文件涵盖了 AI 技术在安全控制方面的多个层面和维度，包括但不限于系统架构与组件、数据采集与处理、算法模型与安全机制、人机交互与用户体验、合规性与伦理考量等，同时明确了《智能 AI 安全控制系统技术规范》的技术内容。主要技术内容旨在确保智能 AI 安全控制系统的安全、可靠和合规性，提升用户体验和满意度。

五、重大分歧意见的处理经过和依据

本标准起草过程中无重大分歧。

六、贯彻标准的措施建议

标准的价值在于实践，唯有得到有效实施方能展现其效用，否则再完善的标准也只能是“空中楼阁”，难以发挥其应有的作用。要确保标准的贯彻落实，关键在于执行力度与配套机制，具体策略涵盖：（1）深化宣传推广。借助报纸、电视、广播以及微信、微博等多元化新媒体平台，广泛开展宣传活动，营造积极的社会氛围，为标准的顺利实施打下坚实基础。

（2）强化实施反馈机制。对于标准执行过程中暴露的问题及收集到的反馈意见，需予以高度重视，进行深入的分析与研讨，并据此不断调整和完善标准内容，确保其更加贴合实际需求。

七、废止现行有关标准的建议

本标准不涉及现行标准的废止。

八、其他应予说明的事项

无。

《标准名称》编制组

2025 年 1 月