



中华人民共和国国家标准

GB/T 48324—2026

人工智能 政务大模型系统技术要求

Artificial intelligence—Technical requirements for large-scale model
systems of government

2026-09-28 发布

2027-04-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 系统参考架构 2

6 基础模型要求 4

7 模型能力要求 4

 7.1 语义理解 4

 7.2 内容生成 4

 7.3 文本问答 4

 7.4 图像理解 5

 7.5 语音交互 5

 7.6 图文处理 5

 7.7 任务规划 5

8 模型工具要求 5

 8.1 知识管理 5

 8.2 模型微调 5

 8.3 提示词工程 6

 8.4 智能体开发管理 6

9 场景应用要求 6

 9.1 政务服务 6

 9.2 社会治理 7

 9.3 机关办公 7

 9.4 辅助决策 7

10 安全合规要求 7

 10.1 基本要求 7

 10.2 数据安全要求 7

 10.3 模型和系统安全要求 8

 10.4 内容生成安全要求 8

 10.5 监管审核要求 8

11 部署运维要求 8

 11.1 系统部署 8

11.2 系统运维 8

附录 A（资料性） 政务大模型系统建设部署模式 10

 A.1 系统技术路线 10

 A.2 模型调度架构 10

 A.3 系统建设部署模式 10

参考文献 12

前 言

本文件按照 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、人民法院信息技术服务中心、华为技术有限公司、河南省政务大数据中心、北京市大数据中心、华中科技大学、湖南农业大学、青岛市大数据发展管理局、北京市司法局、青岛市大数据中心、浪潮云信息技术股份公司、拓维信息系统股份有限公司、福建省人民政府办公厅电子政务中心、北京华宇信息技术有限公司、大汉软件股份有限公司、北京理工大学、北京邮电大学、北京海纳数聚科技有限公司、山西远大纵横科技有限公司、北京中百信信息技术股份有限公司、阿里云计算有限公司、中电科大数据研究院有限公司、北京兴云数科技术有限公司、昆仑数智科技有限责任公司、武汉金山办公软件有限公司、北京百度网讯科技有限公司、数字青岛建设有限公司、华为云计算技术有限公司、北京金山办公软件股份有限公司、广电运通集团股份有限公司、国投智能信息科技股份有限公司、华信咨询设计研究院有限公司、讯飞智元信息科技有限公司、中移雄安信息通信科技有限公司、中关村科学城城市大脑股份有限公司、北京移动系统集成有限公司、中国经济信息社有限公司、人民中科(北京)智能技术有限公司、新华三技术有限公司、浙江省质量科学研究院、智慧足迹数据科技有限公司、福昕鲲鹏(北京)信息科技有限公司、北京华电园信息技术有限公司、无锡市市域社会治理现代化指挥中心、数集(青海)科技有限公司、上海金桥信息股份有限公司、华中师范大学、以萨技术股份有限公司、云赛智联股份有限公司、量安科技(北京)有限公司、南京安通杰科技实业有限公司、北京致远互联软件股份有限公司、南京安夏电子科技有限公司、永中软件股份有限公司、中科信控(北京)科技有限公司、可码科技(江苏)有限公司、园测信息科技股份有限公司、四川极速动力科技有限公司、进迭时空(杭州)科技有限公司、江西微博科技有限公司、中国口岸协会口岸科技应用分会、湖南科创信息技术股份有限公司。

本文件主要起草人：王雷、王晓燕、相福民、陈涛、廖方旭、于浩、李洋、崔昊、衣军成、彭革非、顾晓光、陈璐、林文河、明承瀚、郑佳佳、赵江涛、康丽丽、金震宇、王树良、王友奎、张旭、林佳华、孙传兴、胡璐锦、卢学哲、何运昌、曹扬、刘海军、尚云云、包树南、张英博、郑子木、闫石、吴涛、冯晓蒙、杨旭、阙锦龙、赵学健、陈士星、郑庆国、邢立立、平凡、杨光、秦晓鲁、万晓兰、章古月、施含章、张治、董艳会、杜巍、段尧清、章建兵、钟军、陈豪、龙江涛、梁勇、王翔、杨庄媛、张宏、冯健、武传营、徐浩天、谷敏骏、齐勇、周传健、钱程扬、张小刚、涂震、方明。

人工智能 政务大模型系统技术要求

1 范围

本文件确立了政务大模型系统的参考架构,规定了政务大模型系统的基础模型、模型能力、模型工具、场景应用、安全合规和部署运维等方面要求。

本文件适用于政务大模型系统的建设规划、设计开发、部署集成和持续优化。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/Z 185.1—2026 人工智能 智能体互联 第1部分:总体架构
- GB/T 4657 中央党政机关、人民团体及其他机构代码
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 25647—2026 数字政府 术语
- GB/T 32905 信息安全技术 SM3 密码杂凑算法
- GB/T 32907 信息安全技术 SM4 分组密码算法
- GB/T 32918 信息安全技术 SM2 椭圆曲线公钥密码算法
- GB/T 41867—2022 信息技术 人工智能 术语
- GB/T 45288.1—2025 人工智能 大模型 第1部分:通用要求
- GB/T 45396 数据安全技术 政务数据处理安全要求
- GB 45438 网络安全技术 人工智能生成合成内容标识方法
- GB/T 45654—2025 网络安全技术 生成式人工智能服务安全基本要求
- GB/T 45674 网络安全技术 生成式人工智能数据标注安全规范
- GA/T 2380 信息安全技术 网络安全等级保护数据安全基本要求

3 术语和定义

GB/T 41867—2022 界定的以及下列术语和定义适用于本文件。

3.1

大模型 large-scale model

基于大量数据训练得到,具有复杂计算架构,能处理复杂任务,且具备一定泛化性的深度学习模型。

[来源:GB/T 45288.1—2025,3.1]

3.2

智能体 agent

感知环境,并主动采取行动以实现特定目标的实体。

[来源:GB/Z 185.1—2026,3.1]