

ICS 35.240.01

CCS L76

团 体 标 准

T/CAACCHINA 005-2026

生成式引擎优化 (GEO) 第 5 部分：服务流程合规与安全要求

Generative Engine Optimization (GEO) — Part 5: Service process
compliance and security requirements

2026-09-09 发布

2026-09-10 实施

中国商务广告协会 发 布

目次

目次..... II

前言.....IV

引言..... V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

 3.1 生成式引擎优化 generative engine optimization (GEO) 1

 3.3 GEO 服务商 GEO service provider 2

 3.4 委托方 principal 2

 3.5 黑帽 GEO black-hat GEO 2

 3.6 语料投毒 corpus poisoning 3

 3.7 正向优化 positive optimization 3

 3.8 高合规要求行业 high - regulated industries 3

4 服务总体要求 3

 4.1 基本原则 3

 4.2 可审计要求 4

 4.3 服务边界要求 4

5 服务流程要求 4

 5.1 委托方准入与需求洽谈 4

 5.2 合同与服务边界确认 5

 5.3 业务材料审核 5

 5.4 内容生产要求 6

 5.5 内容可信传播 6

 5.6 评估与测量 7

 5.7 风险处置 7

6 服务安全要求 7

 6.1 信息与内容安全 7

 6.2 数据与个人信息安全 8

6.3 技术与工具安全 8

6.4 商业伦理与竞争安全 9

6.5 过程治理与责任安全 9

7 组织与管理要求9

 7.1 制度建设9

 7.2 组织与人员要求 9

 7.3 流程可追溯要求 10

8 负面行为分级处置要求 10

 8.1 一般违规10

 8.2 严重违规10

 8.3 重大违规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》给出的规则起草。

本文件是《生成式引擎优化（GEO）》系列标准的第 5 部分。该系列标准包括以下部分：

- 第 1 部分：通论及术语与定义；
- 第 2 部分：服务商评估规范；
- 第 3 部分：计价、评估与测量规范；
- 第 4 部分：可信语料规范；
- 第 5 部分：服务流程合规与安全要求。

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。

本文件由中国商务广告协会提出并归口。

本文件起草单位：北京清蓝智汇科技有限公司、阳狮集团、广东因赛品牌营销集团股份有限公司、上海智推时代科技有限公司、上海明堂文化传播有限公司、武汉当夏科技有限公司、耐特康赛网络技术（北京）有限公司、浙文互联集团股份有限公司、芜湖小象园教育科技有限公司、北京深演智能科技股份有限公司、钛镁时代（上海）人工智能科技有限公司、无限增长(北京)智能科技有限公司、北京特比昂科技有限公司、北京优力互动数字技术有限公司、北京杉数智能科技有限公司、薯道电子科技（上海）有限公司、微梦创科网络科技（中国）有限公司、杭州盖立克思人工智能有限公司、深圳智汇蓝媒科技有限公司、苏州闻道网络科技股份有限公司、南京小裂变网络科技有限公司、海知见信息技术（北京）有限公司。

本文件主要起草人：王立新、仲佳伟、黄疏雨、刘文明、杨一舟、鲁扬、毛桂荣、尚晶、张豪、马小婷、周日、张国鹏、李文哲、蔡晓旭、吉晨亮、魏倩、苗建旺、吕虎军、展萌萌、王曦、荆雷、温雅、周斌斌、林煌滨、袁学文、张东晴、周蕾、谭北平、李浩宇、张慧。

本文件主要审查人：丁俊杰、陈徐彬、吴明辉、吴默、陈忠伟、任鹏、全佳欣、李丹、严禧汶、唐兴通。

引 言

生成式人工智能技术的快速发展深刻改变了信息获取与传播的方式，生成式引擎优化（GEO）作为提升真实、合法、准确信息在智能问答环境中可识别性的新型服务形态，日益受到行业关注。为引导 GEO 服务规范有序发展，防范信息失真、虚假传播、数据滥用和模型生态污染等风险，特制定本文件。

本文件旨在建立 GEO 场景下服务流程的整体标准和安全要求，构建标准化的 GEO 服务体系及安全体系。主要用于评估 GEO 整体标准的达成率及安全达标率，由 GEO 服务商自评，或广告主/GEO 委托方抽样检测，或第三方机构抽样评估等。

本标准与 GEO 团体标准体系内其他标准的关系如下：与通论及术语与定义（第 1 部分）的术语与定义保持对齐；与服务商评估规范（第 2 部分）的服务商能力评估要求对接；与计价、评估与测量规范（第 3 部分）的服务交付和测量规范衔接；与可信语料规范（第 4 部分）的语料安全与合规要求对齐。

生成式引擎优化（GEO）第 5 部分： 服务流程合规与安全

1 范围

本文件规定了生成式引擎优化服务在服务流程、安全管理、风险处置、数据保护、内容审核、服务记录和责任追溯等方面的要求。

本文件适用于生成式引擎优化服务商开展生成式引擎优化服务活动，也可委托方、第三方服务机构、行业组织和相关评估机构开展服务管理、风险评估和行业自律提供参考。

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。凡是注日期的引用文件，仅该日期对应的版本适用于本文件；凡是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/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

TC260-005 人工智能应用伦理安全指引 1.0

3 术语和定义

下列术语和定义适用于本文件。

3.1 生成式引擎优化 generative engine optimization (GEO)

通过系统性的技术与内容策略，增强数字内容在生成式 AI 搜索引擎结果中的可见性、准确性和可信度的优化活动。

注 1：GEO 概念由 Aggarwal 等人于 2023 年在论文《GEO: Generative Engine Optimization》（arXiv:2311.09735）中首次系统性提出。

注 2：GEO 的核心目标是让内容在生成式引擎响应中被发现、被引用、被推荐。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.2]

3.2 生成式引擎优化合规 GEO compliance

生成式引擎优化服务在全生命周期中保持合法、真实、透明、可审计、可追溯，并防范各类风险的状态。

注 1：防范的风险包括信息失真、虚假或误导性传播、数据和个人信息泄露、知识产权和商业秘密风险、不正当竞争、模型生态污染、用户权益受损以及公共利益受损等。

注 2：实现该状态的措施包括内容审核、数据保护、技术管理、商业伦理约束、过程治理和责任追溯等。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.4]

3.3 GEO 服务商 GEO service provider

向品牌主或代理机构提供 GEO 相关服务的具有独立法人资格的企业或机构。

注：服务范围可涵盖策略咨询、技术工具提供、内容生产与优化、效果监测与分析、语料管理等一个或多个领域。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.10]

3.4 委托方 principal

基于服务协议接受 GEO 服务商提供的生成式引擎优化服务的组织或个人。

注：委托方通常指具有品牌推广需求的品牌主、广告主或其代理机构。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.12]

3.5 黑帽 GEO black-hat GEO

以操纵、污染、伪造、欺骗或恶意竞争为目的，绕过平台安全机制恶意影响人工智能输出结果的行为。

注 1：典型手段包括利用虚假内容、异常分发、语料投毒、提示词攻击、刷量刷评、伪造信源、恶意贬损竞品等方式。

注 2：依法依规开展的广告投放、公关传播、媒体发布、KOL/KOC 内容合作等正常商业传播行为，在内容真实、合法且不存在欺骗性操纵的情况下，不属于异常分发或黑帽 GEO。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.6]

3.6 语料投毒 corpus poisoning

通过批量注入虚假、误导性、低质量或恶意操纵性内容，干扰生成式 AI 模型认知与输出的违规行为。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.5]

3.7 正向优化 positive optimization

以提升内容的语义清晰度、结构完整性、机器可读性和用户价值为目标，通过合法、合规、符合平台规则的方式开展的优化活动。

注：区别于黑帽 GEO 等违规操纵行为。

3.8 高合规要求行业 high - regulated industries

涉及公共安全、人身财产、生命健康、社会稳定、公众重大利益的垂直行业领域。

[来源：T/CAACCHINA 001-2026，通论及术语与定义 3.1.7]

4 服务总体要求

4.1 基本原则

GEO 服务目标限定于提升真实、合法、准确、权威信息在生成式人工智能平台中的可识别性、可理解性、可引用性和推荐适配性，不应以操纵模型输出结果为目的。

服务商应建立覆盖委托方准入、材料审核、内容生产、技术适配、内容投放、效果监测、风险处置和数据安全的全过程管理机制。

服务商开展 GEO 服务，应遵循以下原则：真实可信、依法合规、公平竞争、用户价值导向、透明可追溯、技术向善。

- a) **真实可信：**所有信息客观真实，产品服务与承诺一致，杜绝欺诈误导；
- b) **依法合规：**严格遵守法律法规与行业规范，建立内部合规体系；
- c) **公平竞争：**通过正当手段竞争，反对垄断与不正当竞争行为；
- d) **用户价值导向：**以用户需求为出发点，聚焦解决真实痛点，创造长期价值；

- e) **透明可追溯**: 清晰披露关键信息, 全流程记录数据处理行为, 建立问题溯源机制;
- f) **技术向善**: 技术服务人类福祉, 防范技术滥用, 推动创新与伦理协调。

4.2 可审计要求

服务商应确保关键服务节点具备完整记录、责任主体和证据留存, 形成可复核、可追踪、可审计的服务链条。

服务过程中形成的审核记录、投放记录、监测结果、优化方案、整改措施和效果报告, 应明确数据来源、时间范围、执行主体、操作内容和复核结果。

对于人工智能辅助生成的内容、分析结果和报告, 应保留生成记录、人工审核记录及最终确认版本。

4.3 服务边界要求

服务商不应承诺“绝对控制模型输出”“百分之百霸屏”等超出事实依据和技术边界的效果。

服务商应在合同、方案和对外沟通中明确服务范围、执行周期、责任边界、交付内容、验收方式和不可承诺事项, 并设置“不可承诺事项清单”作为合同附件。

5 服务流程要求

5.1 委托方准入与需求洽谈

5.1.1 委托方主体核验

服务商应在服务启动前完成委托方主体资格核验。核验内容包括营业执照、行业许可、经营范围、信用记录和授权关系等。

涉及高合规要求行业的, 应执行强化审核机制, 并核验行业许可、备案文件或广告审查批准文件。

服务商应建立委托方风险等级管理制度, 对高合规要求委托方实施强化审核、重点监测和全过程管理。

不应为存在重大违法违规记录、主体身份异常或存在严重失信行为的委托方提供 GEO 服务。

5.1.2 需求确认

服务商应与委托方明确优化目标、预算、时间安排、目标平台、目标用户、现有内容资产、内容边界、竞品提及规则、是否使用人工智能辅助生成内容、效果评估与测量指标和风险处置机制等事项，形成需求确认文档。

服务商不应接受以虚假传播、误导用户、不正当竞争、规避监管或破坏平台规则为目的的服务需求。

5.2 合同与服务边界确认

合同应明确服务范围、数据所有权、合规责任，并包含黑帽 GEO 禁止条款。

合同或项目文件应包括但不限于：

- a) 服务范围、服务周期、交付内容和验收方式；
- b) 数据权属和使用边界；
- c) 内容审核责任和广告标识责任；
- d) 知识产权和商业秘密保护；
- e) 分包合作安排及风险处置机制；
- f) 不可承诺事项清单。

5.3 业务材料审核

服务商应对委托方提供的主体信息、产品信息、技术资料、资质证明、检测报告、专家观点、用户评价和授权文件进行真实性、合法性和完整性审核。

必要时，通过公开信源、第三方证明文件或权威机构材料进行交叉核验。

不应使用虚假、误导、侵权、未经授权或无法证明真实性的业务材料。

对存在瑕疵、授权不完整或真实性存疑的材料，应要求委托方补充证明、限期整改或退回处理。

5.4 内容生产要求

5.4.1 策略制定

服务商应基于资料研读与目标拆解，识别产品核心卖点、差异化价值、风险点及内容缺口，并与委托方共同确定优化目标、目标平台、核心问题域及可量化指标。

5.4.2 内容开发

服务商可按问题矩阵生产结构化内容，包括 FAQ、专家解读、数据报告等形式，并确保信息真实性、合法性和品牌一致性。

内容生产应围绕真实信息、可信信源和用户需求开展，采用正向优化方式，不得通过提示词注入、关键词堆砌、伪造权威背书、隐藏文本或其他黑帽技术手段干扰模型输出结果。

5.4.3 内容审核与发布

使用人工智能辅助生成内容的，应开展人工事实核验、逻辑复核和安全审查，未经审核的人工智能生成内容不得直接对外发布。

内容生产过程应保留初稿、修改稿、审核意见、定稿版本和发布时间等记录。

5.5 内容可信传播

服务商应优先通过委托方官方渠道、权威媒体、专业平台、行业组织和可信内容平台开展分阶段、合规化传播。

内容投放应遵循自然、合理、渐进的信息传播节奏，不得实施恶意群发、僵尸账号矩阵运营、异常刷量或语料轰炸等违规行为。

涉及商业推广、付费合作或广告发布的内容，应依法显著标注“广告”“商业合作”等标识。

投放后应建立巡查机制，及时发现并处置链接失效、内容篡改、违规传播、广告标识缺失和异常传播等问题。

5.6 评估与测量

服务商应建立覆盖服务全过程的评估与测量机制，对优化结果的真实性、有效性、稳定性和合规性进行持续跟踪。

监测指标应具备可量化、可复核和可解释性，不应伪造数据、篡改结果、夸大效果或编造监测报告。

效果分析应综合考虑市场事件、平台算法变化、模型版本更新、媒体传播和竞品活动等因素，不应将全部变化简单归因于 GEO 服务。

服务期间，如发生平台算法调整、模型版本更新、排名异常波动等造成服务效果异常的情况，服务商需在约定时限内主动通知委托方，阐明异常原因并提供应对方案。

测量结果应形成周期性报告，并保留原始数据、截图、时间记录和计算依据。

5.7 风险处置

发现违法违规、虚假误导、侵权、数据泄露或存在重大风险的信息时，服务商应立即启动风险处置机制。

风险处置措施包括但不限于暂停服务、停止传播、清理问题内容、通知委托方、补充说明、整改复核和重新审核。

委托方要求实施违法违规优化行为的，服务商应拒绝执行；情节严重的，可终止合作并保留相关记录。

6 服务安全要求

6.1 信息与内容安全

服务商应建立内容事实核验机制，对品牌卖点、产品参数、行业标准、资质认证、引用数据、第三方评价、榜单排序和竞品比较进行必要核查。

涉及排名、推荐、评分、榜单、横向比较的内容，应明确比较依据并留存原始数据来源和分析过程，不宜使用缺乏依据的绝对化或误导性表述。

对人工智能辅助生成的文字、图片、视频或其他内容，应建立人工复核机制，重点核查事实真实性、知识产权、虚构信息和夸大表述等风险。

6.2 数据与个人信息安全

服务商应优先使用公开、合法、授权或委托方确认可使用的数据和资料，不应使用非法获取、未经授权、来源不明或违反平台规则的数据。

对委托方提供的非公开商业信息、产品策略、消费者洞察、竞品策略和内部资料，应按照保密信息进行管理，不应超出约定服务目的使用，不得用于其他客户知识库训练、跨项目复用。服务合同到期终止后，服务商应删除语料，出具数据销毁确认单。

若监测工具涉及用户搜索行为、账号信息、设备信息、位置或其他可识别信息，应纳入个人信息保护管理，明确收集目的、最小必要、保存期限、访问权限和删除机制。

不应将委托方资料、用户数据或未公开商业信息直接用于未经授权的模型训练、第三方共享或其他项目复用。

6.3 技术与工具安全

监测工具、抓取工具、内容生成工具、分发工具和评估工具应具备权限控制、日志留存、异常处理和供应商管理机制。

工具应记录关键操作和评估依据，包括监测时间、关键词、平台、抓取结果、索引源、版本变化和人工调整记录，确保结果可复核、可追溯。

若使用第三方工具或供应商参与关键词监测、内容生成、数据抓取或分发，应建立供应商尽调、权限管理、数据处理协议、保密义务和安全事件响应机制。

对人工智能生成内容或自动化内容生产工具，应保留提示词、生成版本、人工修改记录和最终发布版本。

6.4 商业伦理与竞争安全

不应通过虚假交易、虚假评价、虚构用户体验、虚假榜单、虚假评分等方式，为委托方制造生成式人工智能可抓取的误导性证据。

不应编造、传播或指使他人传播关于竞争对手的虚假或误导性信息，以影响生成式人工智能系统中的竞品描述、排序或推荐结果。

不应通过低质内容网络、语料轰炸、语料投毒或其他方式污染生成式信息生态。

对竞品比较、榜单排名和推荐理由等内容，应遵循事实依据充分、比较维度明确、不得恶意贬损和不得虚构权威背书的原则。

6.5 过程治理与责任安全

服务商应建立覆盖项目立项、委托方需求确认、风险评估、内容审核、发布审批、工具权限、供应商管理、效果评估、委托方交付和异常处置的治理机制。

服务过程中应建立“委托方确认—内容审核—发布执行—效果监测—复盘纠偏”的闭环流程，并保留必要记录。

对高合规要求行业、高合规要求内容、高合规要求表达和高合规要求竞品比较，应设置更严格的审核机制。

7 组织与管理要求

7.1 制度建设

服务商应建立覆盖服务执行、内容审核、数据安全、风险处置和负面行为防控的管理制度。

制度内容应至少包括服务行为规范、审核流程、风险分级、负面行为清单、整改机制、责任追溯机制和投诉处理机制。

7.2 组织与人员要求

服务商应根据业务规模配置项目管理、内容审核、技术支持、数据安全、风险控制和委托方服务等岗位或能力模块。

合规审查岗位与服务执行岗位宜相对分离，避免同一人员同时承担内容生产、审核和验收职责。

新入职人员、外包服务人员和高合规要求行业项目参与人员，应完成专项培训并通过内部考核后方可参与项目执行。

7.3 流程可追溯要求

服务商应建立全流程日志留存机制，完整记录委托方资质、业务材料、审核过程、优化内容、投放渠道、监测结果、整改记录和责任主体等关键信息。

服务日志、审核记录、发布记录和监测报告等资料，自服务终止之日起保存期限宜不少于三年；法律法规另有规定的，从其规定。

服务商宜采用元数据标签、时间戳、数字水印、电子签名或其他技术手段，保障服务链路可追溯、内容来源可核验、关键数据不可篡改。

8 负面行为分级处置要求

8.1 一般违规

包括但不限于服务记录不完整、流程执行存在轻微瑕疵、非核心内容表述不规范、档案归档不及时和监测记录存在一般性缺漏。

服务商应在 7 个工作日内完成整改，补充相关凭证和记录，经复核通过后方可继续执行相关服务。整改复核记录应归档保存。

8.2 严重违规

包括但不限于广告标识缺失、特殊行业宣传内容不符合监管要求、未经证明使用比较性或绝对化表述、违规使用第三方内容或数据，以及未按规定完成审核即对外发布内容。

服务商应立即暂停相关服务，下架违规内容，启动内部问责机制。整改复核通过后方可恢复服务。同类违规在整改完成后 12 个月内重复发生的，应升级为重大违规处置。

8.3 重大违规

包括但不限于语料投毒、语料轰炸、伪造权威信源、恶意贬损竞品、数据造假、隐私泄露、提示词攻击或绕过平台安全机制，以及伪造监测结果或效果报告。

服务商应立即终止相关服务，固定并留存证据（包括电子数据、系统日志、操作记录等），启动应急处置机制。涉嫌违法犯罪的，依法移交相关部门处理。

参考文献

- [1] 《中华人民共和国网络安全法》[Z].
- [2] 《中华人民共和国数据安全法》[Z].
- [3] 《中华人民共和国个人信息保护法》[Z].
- [4] 《中华人民共和国广告法》[Z].
- [5] 《中华人民共和国反不正当竞争法》[Z].
- [6] 《生成式人工智能服务管理暂行办法》[Z].