政务数据接口安全风险
人工智能识别技术规范

编制说明

《政务数据接口安全风险人工智能识别技术规范》

标准编制组

2026 年9月

目录

一、工作简况

（一）任务来源

为贯彻落实《国务院关于深入实施“人工智能+”行动的意见》（国发〔2025〕11号）关于“建立健全人工智能技术监测、风险预警、应急响应体系”的文件要求，以及《中华人民共和国数据安全法》《中华人民共和国网络安全法》《数字中国建设整体布局规划》等政策要求，规范政务数据共享接口监测能力建设，提升政务数据流通安全监管水平，制定政务数据接口安全风险人工智能识别的相关技术规范，对政务数据共享接口的人工智能辅助监测体系、技术能力及实施方法进行规范，为各级政务单位开展接口安全监测建设提供统一技术参考和实施依据，特提出制定《政务数据接口安全风险人工智能识别技术规范》团体标准。

根据《关于〈政务数据接口安全风险人工智能识别技术规范〉等两项团体标准的立项公告》（粤政务协会〔2026〕12号）相关要求，该团体标准由广东省数字政务协会负责归口与发布，由领信数科信息技术有限公司牵头负责标准编制工作。

（二）起草单位

本标准的主要起草单位拟包括：广州市数字政府运营中心、江门市大数据管理中心、梅州市大数据管理中心、潮州市机构编制研究与事务中心、领信数科信息技术有限公司、广东机场白云信息科技股份有限公司、广东交通职业技术学院、广州卫生职业技术学院共8家企事业单位。

二、目的和意义

随着数字政府建设的深入推进，各级政府部门依托标准化数据接口（API）实现跨部门、跨层级的数据共享与业务协同，大量政务业务通过 API 接口进行调用与数据交换，接口已成为政务数据流通的重要通道。

在政务数据共享规模持续扩大的背景下，接口调用数量与复杂度不断提升，传统基于规则的安全监测方式难以全面识别复杂业务场景中的异常行为，主要体现在：**一是**政务 API 调用涉及不同部门、不同业务系统及多类数据资源，接口访问行为呈现多主体、多路径、高频调用的特点，规则匹配难以覆盖合理调用与异常调用的全部边界；**二是**部分异常行为在技术层面表现“正常”（如返回正常状态码、携带合法令牌），但在业务语义层面可能存在数据滥用、越权访问、异常时段批量调用等风险，传统以技术特征为主的监测手段难以识别其业务语义层面的安全隐患。

随着人工智能技术特别是大模型语义理解能力的快速发展，利用人工智能技术对 API 接口行为进行语义识别、业务理解和行为分析，能够有效提升政务数据共享过程中的风险识别能力，推动安全监测从“技术规则匹配”向“业务语义理解”转变，实现异常调用的智能发现与风险研判。

目前国内与政务数据接口安全相关的标准主要包括 GB/T 37988—2019《信息安全技术数据安全能力成熟度模型》（DSMM）、GB/T 22239—2019《信息安全技术网络安全等级保护基本要求》，以及 GB/T

39477—2020《信息安全技术政务信息共享数据安全技术要求与安全评估方法》、GB/T 46796—2025《数据安全技术数据接口安全风险监测方法》等。上述标准主要**从数据安全管理和网络安全防护，以及接口安全风险监测方法等角度提出要求，但针对利用人工智能技术（语义理解、行为分析）开展政务数据共享接口安全风险识别，尚缺乏专门的技术规范**。

为贯彻落实《政务数据共享条例》（国务院令809号，2025年8月1日施行）关于“加强政务数据共享安全保障”的要求，以及国家关于加快数字政府建设、推动人工智能与政务服务深度融合的决策部署，制定《政务数据共享服务接口安全风险人工智能识别技术规范》将填补政务数据共享接口安全风险人工智能识别能力方面的标准空白，为各级政务单位开展政务数据共享服务接口安全风险人工智能识别系统的设计、建设、运行、测试与评估提供统一技术依据。

三、编制原则

本标准制定遵循以下原则:

1.协调性

本标准严格遵循国家、广东省及各地市各级法律法规与宏观政策导向，密切结合现代信息技术发展现状与广东省数字政府改革建设相关要求。在充分吸纳《广东省公共数据管理办法》（省政府令第290号）、《广东省公共数据资源授权运营管理办法》（粤政数〔2026〕9号）、《广东省公共数据资源登记管理实施细则（试行）》（粤政数〔2025〕21号）及《关于加快公共数据资源开发利用的实施意见》

等政策文件精神的基础上，本标准紧扣政务数据共享服务接口安全运营对风险识别提出的“高标准、高要求”，制定相关技术规范；并在编制过程中始终与国家现行政策体系、上位标准规范（如GB/T 39477、GB/T 22080、GB/T 22239、GB/T 35273、GB/T 37988、GB/T 43697、GB/T 45654、GB/T 46796等）及行业发展趋势保持协调统一。本标准与广东省现行公共数据管理制度重点条款的对齐说明，以及主要条款与上位标准规范的对应关系，见本编制说明相关章节，以确保标准落地时有据可依、上下贯通。

2.目标向导

本标准以“应用人工智能技术增强政务数据共享接口安全风险识别能力”为核心目标，聚焦保障政务数据机密性、完整性、可用性和合规使用的根本宗旨。编制中坚持问题导向，围绕政务数据共享服务接口在接口注册接入、身份鉴别与访问控制、数据传输与暴露、调用注入与攻击、调用滥用与失控、跨接口汇聚关联与重识别、审计与可追溯等环节面临的实际风险（如未鉴权与弱鉴别、越权调用、明文传输与脱敏失效、注入攻击与恶意载荷、调用滥用与爆破、关联推断与重识别、审计缺失与不可追溯等），明确总体框架、系统构成、能力要求、技术要求与证实方法，确保标准条款有的放矢、直指痛点，避免泛化空泛。

3.实用性

本标准在编制过程中，广泛结合广东省数字政府建设发展实际情况，以及现有政务云平台运营、安全运营中心（SOC）接口安全监测、

政务数据分类分级与共享开放、公共数据授权运营等已开展的实践基础，从总体框架、系统构成、能力要求、技术要求、证实方法等方面进行规范。编制组进行了充分的调查研究与必要验证，吸收一线运营单位、首席数据官（CDO）体系及授权运营机构的实践经验，保障标准条款设置合理可行、切实可用，具有良好的实用性和可操作性。

4.可行性

本标准注重落地实施的可行性。条款设置遵循“人机协同、人负其责”的务实路径，区分 L1 自动处置、L2 人工研判、L3 应急响应（必要时应急关停）的分级处置机制，既鼓励 AI 赋能提效，又明确最终处置决策由具备相应权限的人员作出，避免脱离实际的无条件自动化。对模型上线前的测试验证、上线后的性能监测与重训、退役后的版本归档等均给出可执行的闭环要求，并以 GB/T 37988—2019《数据安全能力成熟度模型》的方法论作为能力评价依据，使标准可度量、可考核、可改进。

5.规范性

本标准严格按照 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》确立的规则进行编写。编制组在起草阶段即对标该导则，对标准文本的要素构成、编排格式及表述逻辑进行规范，确保本标准在结构与形式上与国家标准化文件的基本规则保持一致，术语和定义、缩略语、引用文件等要素齐备、表述严谨。

6.公开透明

本标准的编制遵循团体标准公开、透明的工作程序，编制过程向

社会相关方公开征求意见，充分吸纳政务部门、运营单位、行业专家与社会各界的建议。同时，标准内容本身强调接口风险识别与处置全过程“可审计、可追溯、留痕可查”，并要求运营报告的公开范围与内容按照国家及广东省政务数据共享开放相关规定执行，涉及敏感风险信息、漏洞细节、告警信息的内容脱敏后按权限共享，在保障安全的前提下提升运营的透明度与可监督性。

四、编制过程

1. 标准立项：2026 年 4 月 9 日，经协会审批，该标准项目正式立项，《关于〈政务数据接口安全风险人工智能识别技术规范〉等两项团体标准的立项公告》（粤政务协会〔2026〕12 号）经协会官网和全国团体标准信息平台公开发布。

2. 成立标准编制组：2026 年 5 月 6 日，协会正式发布公告公开征集参编单位，吸纳了广州市数字政府运营中心、江门市大数据管理中心、梅州市大数据管理中心、潮州市机构编制研究与事务中心、领信数科信息技术有限公司、广东机场白云信息科技股份有限公司、广东交通职业技术学院、广州卫生职业技术学院等单位的专业技术骨干和相关人员组成标准编制组，主要负责标准文本的起草编制任务。在前期资料搜集和初步调研的基础上，形成标准制定工作方案，包括阶段进度安排、关键时间节点、人员工作分工等，并确立了内容大纲。

3. 编制初稿：2026 年 6 月 1 日—2026 年 8 月 21 日，标准编制组根据计划开展标准初稿编制工作，系统查阅了《政务数据共享条例》（国务院令第 809 号，2025 年发布）、《关于构建数据基础制度更

好发挥数据要素作用的意见》（中办发〔2022〕51号）、《生成式人工智能服务管理暂行办法》（国家互联网信息办公室令第15号）、《广东省公共数据管理办法》（广东省人民政府令第290号，2021年发布）、《广东省公共数据资源登记管理实施细则（试行）》（粤政数〔2025〕21号）、《广东省公共数据资源授权运营管理办法》（粤政数〔2026〕9号）等政策文件，以及《数据安全技术数据接口安全风险监测方法》（GB/T 46796—2025）、《网络安全技术生成式人工智能服务安全基本要求》（GB/T 45654—2025）等相关国家标准与技术规范，在充分收集整理基础资料和开展调研论证的基础上，围绕政务数据共享服务接口安全风险人工智能识别的术语定义、总体要求、系统构成、风险识别流程、技术要求与证实方法，对标准框架和相关技术内容反复进行了修改，形成了标准（草案）。

4. 技术研讨:

2026年8月24日，标准编制组在广东省广州市天河区黄埔大道西平云路163号广电平云广场广电科技大厦5楼会议室组织召开标准编制内部研讨会，邀请领信数科信息技术有限公司、广东机场白云信息科技股份有限公司、广东交通职业技术学院、广州卫生职业技术学院等起草代表参与讨论。参会代表基于各自的行业经验，提出了主要修改完善建议如下:

一是风险识别流程框架应与GB/T 46796—2025的精准对接，在原有四阶段（监测准备—风险识别—分析研判—预警处置）基础上增列审计追溯，形成本文件五阶段。

二是新增人工智能能力要素层的内容，解决在人工智能应用时算力、模型、数据三要素应遵循的要求（算力 GB/T 45958/模型 GB/T 45654/数据 GB/T 45652、45674），详细描述外移附录 C（资料性），正文保留引导语。

5. 形成征求意见稿:

2026 年 9 月 15 日，标准编制组在完成标准初稿的基础上，通过内部研讨、组内审稿及定向咨询等方式，针对标准草案中少数存在异议的技术条款与表述进行反复讨论，在充分吸纳合理意见并对文本进行修改完善后，正式形成了标准（征求意见稿）及其编制说明。

五、标准的主要内容

（一）技术内容说明

本标准规定了政务数据共享服务接口安全风险人工智能识别的总体要求、系统构成、识别流程、识别要求与证实方法。本标准拟适用于政务数据共享服务接口安全风险人工智能识别系统的设计、建设、运行与评估，也可供主管（监管）部门实施相关安全监督管理时参考。

（1）总体要求：描述了人工智能识别政务数据共享服务接口安全风险活动应遵循的总体原则。

（2）系统构成：描述了政务数据接口安全风险人工智能识别系统的四层构成——数据采集层、人工智能能力要素层、识别分析层、处置协同层，覆盖监测、识别、研判、处置闭环。

（3）识别流程：描述了以监测准备、风险识别、分析研判、预警处置、审计追溯五个阶段为主线的闭环识别流程，阶段划分参照

GB/T 46796—2025 规定的数据接口安全风险监测闭环；明确接口安全风险在各阶段的集成，并给出风险识别流程图；审计追溯结果反馈优化识别基线、阈值与策略，形成流程闭环。

（4）技术要求：描述了针对鉴权与访问控制、传输与数据暴露、注入与攻击、滥用与失控、汇聚关联与重识别、审计与可追溯等风险，以及数据合规要求、责任与分级处置要求的技术识别要求。

（5）证实方法与能力核查：对应第 8 章各项识别要求逐条给出证实方法，形成“识别要求—证实方法”逐条配对（第 9 章）；并以附录 B（典型安全风险类型与识别能力核查表，含风险类型、编号、风险类、对应条款、风险项、技术要求条款、证实方法、相关标准编号等）与附录 C（风险识别流程各阶段输出材料模板）作为系统评估、验收与持续优化的核查依据。

（二）编制总体思路

本标准的编制以“利用人工智能技术增强政务数据共享服务接口安全风险识别能力”为主线，坚持问题导向、目标导向与可落地导向相结合，整体思路可概括为“**一个中心、两条主线、六类风险、三层闭环”，具体如下：**

1.一个中心

始终围绕“政务数据共享服务接口”这一政务数据流通的最小可控单元，而不是围绕网络域、系统域或安全监测产品。这意味着标准回答的是“数据通过什么接口、被谁调用、以什么方式交换才安全”，而不是“部署了什么监测设备”。接口是政务数据跨部门、跨层级共

享的必经通道，对其调用行为进行人工智能识别，是政务数据安全运营中最具靶向性、最具可追溯性的切入点。

2.两条主线

横向主线——接口安全风险识别的流程闭环：以“监测准备→风险识别→分析研判→预警处置→审计追溯”五个阶段为主线的闭环识别流程，阶段划分与任务要求对接 GB/T 46796—2025《数据安全技术数据接口安全风险监测方法》规定的监测闭环（在其四阶段基础上增列审计追溯）。

纵向主线——AI 赋能接口风险识别的通用能力：覆盖从数据到处置的四层通用能力，即数据采集底座、人工智能能力要素层（算力/模型/数据三要素）、识别分析能力（UEBA、流量深度检测、GNN 关联推理）、处置协同能力（SOAR 人机协同编排）。纵向主线解决“用 AI 怎么识别”的能力构建问题。

3.六类风险

把横向主线落到的风险对象拆解为 6 类接口安全风险(R1 ~ R6), 每类风险独立成节，分别规定风险点与人工智能识别要求。这样做的考虑是——接口安全风险高度依赖上下文，脱离具体风险类别谈“AI 赋能”会变成技术堆砌，只有落到具体风险类别才能给出可执行的要求：

R1 鉴权与访问控制：越权调用、凭证盗用、非法接口暴露;

R2 传输与数据暴露：明文传输、敏感字段回传、过度采集;

R3 注入与攻击：参数注入、越权遍历、批量爬取;

R4 滥用与失控：高频调用、资源耗尽、调用行为偏离；

R5 汇聚关联与重识别：跨接口关联推断、去标识化后重识别；

R6 审计与可追溯：日志缺失、操作不可审计、抗抵赖不足。

注：数据合规要求（8.1）与责任分级处置（8.8）为贯通性要求，不单独计入六类风险，但在每一风险类别的识别过程中均需落实。

4.三层闭环

运营闭环：识别→研判→处置→复盘→优化。五阶段流程对应识别—研判—处置，复盘—优化由审计追溯与过程控制驱动，形成持续改进的运营闭环。

责任闭环：接口提供方（数源部门）、政务数据共享平台运营方、安全运营中心（SOC）识别系统运营团队、公共数据主管部门（政务数据管理机构）各司其职；分级处置 L1/L2/L3 落实“人机协同、人负其责”，最终处置决策由具备相应权限的人员作出。

评价闭环：以附录 B 能力核查表（7 列 40 项）与第 9 章证实方法开展能力评估，对标 GB/T 37988—2019《数据安全能力成熟度模型》的方法论；并结合 AI 模型全生命周期管理（上线前测试验证、上线后性能监测与重训练、退役后版本归档）驱动识别能力在成熟度框架下持续螺旋上升。

（三）主要实验（验证）情况分析/主要核心量化指标的设定

标准中所有核心量化指标均基于行业实践、国标对标与技术可行性综合确定，确保指标“可落地、可验证、无超出现有技术水平的过高要求”，核心指标设定依据如下：

1.审计日志留存期不少于6个月：依据GB/T 46796—2025《数据安全技术数据接口安全风险监测方法》中5.4“过程控制”对监测数据留存的要求，并衔接GB/T 22239—2019《网络安全等级保护基本要求》关于安全审计记录保存期限的规定，结合政务数据共享接口调用的追溯与定责需要确定，作为可核查的下限指标。

2.分级处置三级响应（L1自动处置/L2人工研判/L3应急响应）：依据行业安全编排自动化响应（SOAR）三级处置通行实践，并衔接全国网络安全标准化技术委员会《人工智能安全治理框架》2.0提出的“风险分级、分级治理”原则，将风险按等级对应自动处置、人工研判与应急关停，既鼓励AI提效又确保“人负其责”。

3.接口调用频控阈值（令牌桶/滑动窗口/动态基线限流）：依据GB/T 39477—2020《政务信息共享数据安全技术要求与安全评估方法》中6.2访问控制（会话监视与控制、鉴别失败安全控制）以及GB/T 22239—2019防爆破要求，标准不规定统一固定数值，而是由运营方依接口业务特性设定，保证指标贴合实际、可落地。

4.UEBA行为基线偏离判定阈值：依据YD/T 4246—2023《电信网和互联网数据异常行为监测技术要求与测试方法》对异常行为监测的方法学要求，标准不限定具体算法与固定偏离度，由运营方依历史调用行为建立基线并设定偏离阈值，避免对算法性能提出超出现有技术水平的过高要求。

5.原始数据不出域、可用不可见：依据中办发〔2022〕51号《关于构建数据基础制度更好发挥数据要素作用的意见》(“数据二十条”)

中“原始数据不出域、数据可用不可见”的硬性要求，作为接口监测与风险研判过程必须遵循的合规底线，并通过 GB/T 45230—2025《机密计算通用框架》实现技术落地。

6.监测数据加密、脱敏、备份与到期删除: 依据 GB/T 46796—2025 5.4 对监测数据保护的要求，并衔接 GB/T 35273—2020《个人信息安全规范》、GB/T 45574—2025《数据安全技术敏感个人信息处理安全要求》，对接口监测过程中涉及的个人信息与敏感数据提出可验证的保护指标。

7.识别准确率、召回率等模型性能指标不规定统一固定值: 考虑到政务数据共享接口业务场景差异大、现有技术水平下难以给出“普适硬指标，标准采用”由运营方依业务风险等级设定并持续监测重训练的表述，仅在证实方法中要求提供性能监测记录，避免提出脱离实际的过高要求，确保指标可验证、可改进。

六、知识产权情况说明

本标准不涉及知识产权。

七、与现行相关法律、法规和强制性国家标准的关系

（一）总体关系

本标准属于团体标准（推荐性技术规范），其技术要求在国家现行法律、行政法规、部门规章及强制性国家标准的框架内，对政务数据共享服务接口安全风险的人工智能识别作出细化与补充。依照《中华人民共和国标准化法》，团体标准的技术要求不得低于强制性国家标准；本标准全文未设定任何低于强制性要求的条款，且主动衔接唯

一的强制性引用标准 GB 45438—2025，故与现行法律、法规和强制性国家标准不存在冲突或抵触。

本标准第 2 章规范性引用的 14 项国家标准中，仅 GB 45438—2025 为强制性国家标准，其余均为推荐性国家标准（GB/T），不构成强制约束面，仅作为技术对标与证实依据。

（二）与现行法律的关系

法律	相关条款精神	本标准对应落点	关系
《中华人民共和国数据安全法》（2021）	数据分类分级（第 21 条）、数据安全保护义务（第 27 条）、风险监测（第 29 条）	引用 GB/T 43697—2023 落实接口数据分类分级;第 6 章风险识别流程对接 GB/T 46796—2025 监测闭环;第 7 章六类风险识别落实风险监测义务	一致、细化落实
《中华人民共和国个人信息保护法》（2021）	安全措施含审计、加密、去标识化（第 51 条）、个人信息处理影响评估（第 55 条）	第 6.8 条监测数据脱敏、加密、备份；第 7.7 条审计与可追溯;引用 GB/T 35273—2020、GB/T 45574—2025	一致、场景细化
《中华人民共和国网络安全法》（2017）	网络安全等级保护（第 21 条）	引用 GB/T 22239—2019 等级保护基本要求作为接口运行环境安全基线	一致
《中华人民共和国密码法》（2020）	商用密码应用与安全（第 22、27 条）	第 6.8 条提出监测数据"加密传输与存储"，其加密实现应依《密码法》采用商用密码合规应用	协调、不冲突

（三）与行政法规、部门规章的关系

法规 / 规章	性质	本标准对应落点	关系
《政务数据共享条例》（国务院令第 809 号，2025-08-01 施行）	行政法规（本标准直接适用上位依据）	本标准紧扣条例关于政务数据共享安全保障的要求,填补"利用人工智能技术识别接口安全风险"的能力空白；第 3.1 条"政务数据"定义直接溯源 809 号第三条	一致、支撑落地
《生成式人工智能服务管理暂行办法》（国家网信办等七	部门规章	第 7.1.5 条要求生成式 AI 研判报告符合 GB/T 45654—2025 与 GB 45438—2025 的标识与安全措施；第 7.8 条落实"人负其	一致、主动衔接

法规 / 规章	性质	本标准对应落点	关系
部门令第 15 号，2023-08-15 施行）		责"责任条款；AI 能力要素层（5.3）对接 15 号关于安全评估、内容标识、责任界定的要求	

（四）与政策文件的关系（导向衔接，不属法规强制层面）

中办发〔2022〕51 号《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）：提出“原始数据不出域、数据可用不可见”。本标准第 7.1.4 条将“数据不出域、可用不可见”作为接口监测与风险研判的合规底线，并通过 GB/T 45230—2025 机密计算实现技术落地。

上述政策文件体现国家数据基础制度与数字政府建设导向，本标准在编制原则、总体要求中与之保持一致，但政策文件本身不进入第 2 章规范性引用。

（五）与强制性国家标准的关系

GB 45438—2025《网络安全技术人工智能生成合成内容标识方法》（强制性）：本标准识别系统在使用生成式人工智能生成风险研判报告或预警内容时，会产出人工智能生成合成内容。第 4.4 条、第 7.1.5 条、第 8.1.5 条已明确要求生成内容满足 GB 45438—2025 的标识方法与安全措施，并在证实方法中审查标识记录。本标准技术要求与该项强制性国标完全衔接，无冲突。

其余引用标准均为推荐性（GB/T），本标准未在其中设定低于其要求的技术指标。

（六）冲突分析结论

1.本标准为团体标准，技术内容在《数据安全法》《个人信息保

护法》《网络安全法》《密码法》《政务数据共享条例》《生成式人工智能服务管理暂行办法》等法律、法规框架内细化，相关强制性底线均被遵守并在条款中落实。

2.本标准唯一强制性引用标准 GB 45438—2025 已在正文（4.4、7.1.5、8.1.5）显式衔接，无抵触。

3.第 2 章规范性引用的 14 项国家标准经全文核查均为现行有效、无废除、无替代，与强制性国标及法规无冲突。

4.结论：本标准与现行相关法律、法规和强制性国家标准不存在冲突，且通过条款显式衔接实现了对强制性要求的落实与对政策导向的支撑。

八、相关国内标准情况简要说明

与本标准较为相关的标准规范包括:

——国家标准:

GB/T 46796—2025《数据安全技术数据接口安全风险监测方法》、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 45652—2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》、GB/T 45674—2025《网络安全技术生成式人工智能数据标注安全规范》、GB 45438—2025《网络安全技术人工智能生成合成内容标识方法》（强制性）等;

——团体标准:

《人工智能智能体内生安全技术要求》（T/ZGCMCA 023-2025）、《生成式人工智能内容安全检测规范》（T/UNP 186-2026）、《人工

智能智能体互操作性接口规范》（T/ZGCMCA 024-2025）、《人工智能大模型数据标注技术要求》（T/ZGCMCA 006-2025）、《人工智能应用安全监测与应急响应规范》（T/BJCSA 08-2025）等。

这些标准主要从数据接口安全风险监测、生成式人工智能服务与训练数据安全、数据标注安全、内容安全检测、人工智能应用安全监测与应急响应等方面进行了规定，但主要侧重于通用人工智能技术能力或应用形态的安全要求，**缺少针对“政务数据共享服务接口”这一特定场景、利用人工智能开展接口安全风险识别的专门规范**。

总体来看，现有标准体系尚未形成针对“**政务数据共享接口+人工智能+安全风险识别**”场景的安全治理能力框架，尤其在大模型语义理解赋能接口行为分析、业务语义层面风险研判、AI 识别与分级处置协同等方面缺乏统一规范。**本标准的制定将填补政务数据共享服务接口安全风险人工智能识别能力方面的标准空白**，为各级政务单位开展政务数据共享服务接口安全风险人工智能识别系统的设计、建设、运行、测试与评估提供统一技术依据。

九、重大分歧意见的处理经过和依据

本标准未产生重大分歧意见。

十、标准性质的建议

本标准作为推荐性标准，属于团体标准，供协会会员和社会自愿使用。

十一、标准实施建议

本标准批准发布实施后，尽快将本标准的批准信息通告编制小组

成员单位及其他有关单位。积极组织本标准的宣传和培训，使涉及政务数据共享服务接口安全风险识别工作的相关单位与管理人员熟悉了解本标准的内容、特点，保证标准的顺利实施，使标准的应用真正落到实处。

为全面掌握本标准的执行情况，鼓励使用单位和相关单位将本标准的执行情况以及所发现的问题及时反馈到归口团体或本标准的起草单位，为标准完善工作做好准备，不断提高标准的科学性、合理性、协调性和可操作性。

十二、其他应说明的事项

无。