

附件

中国—东盟“护航丝路”人工智能安全大赛方案

一、大赛主题

聚焦人工智能算力安全、算法安全、数据安全、应用安全，系统开展全链条安全风险评估与防控，依托创新测评工具、智能监测平台和权威认证服务，构建集评估、监测与认证于一体的人工智能安全服务管理体系。积极服务国家“一带一路”倡议和中国—东盟命运共同体建设，护航广西人工智能产业高质量发展，打造区域性人工智能安全高地。

二、组织机构

主办单位：广西壮族自治区党委网信办、广西壮族自治区大数据发展局、南宁市人民政府

承办单位：中国网络社会组织联合会、奇安信科技集团股份有限公司

协办单位：人民中科（北京）智能技术有限公司、广西网络安全和信息化联合会

三、参赛对象

面向中国和东盟各界开放，支持中国和东盟国家有关头部企业、初创团队、科研院所、高校学生、个人开发者参与，鼓励国内队伍同东盟国家、在桂高校学生联合组队。

每支参赛队伍队长 1 人，团队总人数不多于 5 人，每个参赛作品只可选择一个赛道进行参赛。每支参赛队伍可提交多个作品。

四、赛道说明

（一）算力安全赛道

聚焦 AI 基础设施的算力安全，围绕芯片、异构计算平台、虚拟化调度及边缘设备，构建横跨云边端的一体化算力安全防护体系，保障训练与推理过程的稳定性、可信性与资源使用安全。

（二）算法安全赛道

面向 AI 算法模型的可信计算需求，提升其鲁棒性、抗攻击性、可解释性和公平性，防范模型遭受对抗样本、后门注入、逻辑操控等恶意行为，确保算法输出的可靠性与合规性。

（三）数据安全赛道

围绕 AI 系统从数据采集、清洗、标注、传输到存储与使用的全流程安全治理，特别聚焦东盟语言大模型训练语料的合法性、隐私性与版权合规问题，数据跨境传输的安全问题，构建系统化的数据治理与防护体系。如面向东盟的数据跨境流动场景中，通过注入恶意样本等攻击检验加密能力；打击电信网络诈骗场景中，以伪造视频攻击检验检测与溯源能力。

（四）应用安全赛道

聚焦 AI 在开发、部署、运维和服务阶段的全生命周期安全，融合 AI 应用供应链防护与生成内容识别机制，确保 AI 系统从组件到输出内容的全面可信、可控与可追溯。如第三方组件和 AI

框架的安全评估、环境安全加固、智能运维系统实时监控等场景；AI 生成内容检测、深度伪造识别溯源场景；AI 赋能渗透测试、安全运营、异常行为分析、恶意代码检测分析等网络空间安全防护场景；AI 赋能千行百业场景下的安全监管，特别是面向东盟的跨境物流、智能制造场景下，检验调度算法抗干扰能力、监控与应急响应能力等。

（五）实战攻防赛道

立足国家网络安全战略，聚焦自动驾驶、智能家居、智慧社区等与民生息息相关的 AI 深度应用场景，构建实战化攻防体系。通过网络靶场进行高仿真攻击，检验参赛团队在 AI 模型安全加固、数据隐私防护、算法漏洞对抗等方面的核心能力，推动技术创新与成果转化，筑牢民生安全防线。

五、报名要求

（一）报名渠道：2025 年 7 月 19 日 18 时—8 月 15 日 18 时在智桂通平台（APP 或小程序）报名（链接：<https://enterprises.gxzgt.com:22364/eventplanning/#/>，或扫描下方二维码）



（二）报名材料：《中国—东盟“护航丝路”人工智能安全大赛参赛报名信息表》（报名平台下载，填写团队信息表、作品

介绍、技术路线、应用场景、可实施性及知识产权声明等内容)

(三) 作品提交: 除报名信息表外, 其他可展示作品情况的资料, 如 demo 演示视频、产品详细介绍文档等材料, 也可一并提交, 因数据量太大等原因不方便上传的可在报名表信息表提供下载或在线演示链接。

(四) 作品要求: 必须是原创作品, 未侵犯任何第三方的知识产权, 具有创新性和实用性。

六、时间安排

(一) 启动报名 (2025 年 7 月 19 日—2025 年 8 月 15 日)

发布赛事通知及参赛指南, 全面开放线上报名通道。期间将举办赛前技术说明及推介活动。

(二) 初筛评审 (2025 年 8 月 16 日—2025 年 8 月 31 日)

组织专家团队对报名项目进行合规性审核、赛道匹配度分析及初步质量评估, 筛选出具备落地潜力、技术先进性强的优质项目入围决赛环节。

(三) 专家评审 (2025 年 9 月 1 日—2025 年 9 月 15 日)

开展集中评审, 专家委员会对入围项目进行现场评审、质询讨论打分, 开展实战攻防, 评选出各赛道优秀项目和获奖团队。

(四) 成果转化 (2025 年 9 月中下旬)

赛事设立广西优先落地政策与专项激励机制, 推动优秀项目在广西实现快速孵化与场景落地。借助东博会期间举办的专项成果推介会、技术交流和投资对接活动, 深化与东盟各国政府、产

业园区及企业的合作，促进项目跨境应用与产业链协同共建。

（五）颁奖交流（2025 年 10 月）

举办颁奖典礼，开展技术交流、产品展示、应用对接等系列活动。

七、资源支持与奖励

（一）资源支持

场景支持：优秀项目纳入自治区 AI 安全场景库，优先对接企业落地需求，提供真实业务环境测试机会。

孵化支持：潜力项目推荐人工智能产业基金投资对接，入驻自治区相关产业园享受孵化服务。

（二）平台支持

本次大赛依托中国—东盟人工智能创新合作中心（简称“南 A 中心”）在人工智能政策支持、技术研发、成果展示及产业协同方面的优势，助力优秀成果实现孵化、转化及跨境推广。

（三）奖励方式

本次大赛设立主赛道奖项与特色奖项两大类，按照不同奖项级别，给予相应奖金。项目主要成员（在桂工作）优先纳入广西相关人才支持专项计划，并积极向上级推荐参评国家相关人才项目。获奖项目所在单位若提出申请，可优先考虑获评广西人工智能安全技术支撑单位资格。