



广州供电局

2026 年网络安全技术防护-数字运营

中心-内容安全护栏

技术规范书



目 录

1. 总则	1
1.1. 概述	1
1.2. 定义	1
1.3. 招标范围	2
1.4. 工程保证	2
1.4.1. 组织保证	2
1.4.2. 质量保证	2
1.4.3. 工期保证	2
1.4.4. 项目质保期	2
1.5. 项目标准及规范	3
2. 项目概况	4
2.1. 项目目标	4
2.2. 项目范围	4
3. 项目工作内容	4
3.1. 项目内容	4
3.2. 技术要求	5
3.3. 项目转分包要求	8
3.4. 项目验收与知识产权要求	9
3.5. 服务团队及服务能力	9
3.6. 技术服务要求	10
3.6.1. 服务质量要求	10
3.6.2. 事件响应要求	10
3.7. 项目转分包要求	12
3.8. 网络安全管理要求	12
3.9. 其他要求	13
4. 服务团队优异性表格	14
4.1. 一般服务团队条款/参数	14
4.2. 服务团队优异性表格	15

5. 技术条款/技术参数点对点应答表	16
6. 主要条款/参数优异性表格	18
7. 优选总体方案定义	21
8. 质量保证及售后服务要求	21
8.1. 售后服务总要求	21
8.2. 技术维护支持服务	22
8.3. 技术支持人员要求	22
9. 项目创新评价专项标准	23
10. 违约责任	28
11. 效力说明	28

1. 总则

1.1. 概述

1) 本技术规范书适用于 2026 年网络安全技术防护-数字运营中心-内容安全护栏，本技术规范书的所有解释权归广州供电局。

2) 本技术规范书提出了本次招标项目的技术要求和实施技术指标要求，可供投标人编写投标文件之用。

3) 投标人应按照本技术规范书的要求提供详细、完整的技术投标书。该技术投标书应完全满足或高于本技术规范书要求，对于本技术规范书中的某些部分，投标人如不能满足要求，或有其它替代方案，或有其它修改建议，应在技术投标书中指出其必须进行修改的理由以及与原要求的差别，否则，招标人即认为投标人可以满足本技术规范书的要求。

4) 所有招标人认为是本技术规范书范围所要求而被遗漏的项目，都被认为是包含在本次招标范围内，投标人的报价被视为包含此遗漏项目的报价。投标人可以就投标人认为的遗漏项目提请招标人注意，并详细说明理由。招标人将就此进行澄清。

5) 投标人应保证所提供的所有资料真实、完整、准确无误，否则招标人将有权取消投标人的中标资格，由此产生的一切后果由投标人承担。

6) 投标人必须完整填写“一般服务团队条款/参数”、“服务团队优异性表格”、“技术条款/技术参数点对点应答表表”和“主要技术条款优异性表格”，如发现作假，招标人有权追究投标人责任。

1.2. 定义

1) 招标人：广东电网有限责任公司广州供电局。

2) 投标人：指响应招标、参加投标竞争的法人。

3) 中标人：经过评标，被授予合同的投标人。

4) 本规范书被合同引为附件时，“招标人”权利义务亦为甲方权利义务，“投标人”、“中标人”权利义务亦为乙方权利义务。

5) 当采用非招标方式采购时，“招标人”指采购人，“投标人”指应答人。

1.3. 招标范围

本次招标范围是 2026 年网络安全技术防护-数字运营中心-内容安全护栏。

具体如下：

2026 年网络安全技术防护-数字运营中心-内容安全护栏	采购内容安全护栏，用于支持大模型应用识别、分类、应用评估、使用环境风险评估。
------------------------------	--

1.4. 工程保证

1.4.1. 组织保证

项目团队中必须包含项目经理、实施人员等，按需派驻或上门。

1.4.2. 质量保证

投标人应保证所提供的实施服务满足本技术规范书要求。

1.4.3. 工期保证

项目工期自合同签订之日起至 2027 年 12 月 31 日（因甲方原因或不可抗力需修改工期的，如合同正文另行约定或有其他约定，从其约定）。

1.4.4. 项目质保期

本项目的质保期为系统建设竣工验收合格之日起一年，保质期内投标人需免费为项目提供包含以下系统支持服务：

➤ 电话热线服务

配备有经验的售后工程师接听客服电话，及时响应招标人提出的系统问题。

要求响应时间范围为 7×24 小时。响应速度为 5 分钟以内。

➤ 远程支持

对于客服电话解答不了的问题，由售后工程师通过远程网络连线至主机进行远程支持。

要求响应时间范围为：7×24 小时。响应速度 10 分钟以内。

➤ 现场服务

对出现不能远程解决的问题，或在系统的运行环境不完全成熟的条件下，需要提供售后工程师的上门服务，现场解决问题。

要求响应时间范围为：7×24 小时，响应速度 10 分钟以内，30 分钟到达现场。

1.5. 项目标准及规范

本项目必须遵循以下规范和标准：

- (1) 《中华人民共和国网络安全法》
- (2) 《中华人民共和国密码法》
- (3) 《中华人民共和国数据安全法》
- (4) 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
- (5) 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
- (6) 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）
- (7) 《中国南方电网有限责任公司信息化工作管理规定》
- (8) 《中国南方电网有限责任公司信息化项目预算编制与计算方法（2024 年修订版）》
- (9) 《中国南方电网有限责任公司管理信息系统信息安全保障体系》
- (10) 《中国南方电网有限责任公司管理信息系统安全等级保护标准》
- (11) 《南方电网公司数字化转型和数字南网建设行动方案（2020 年版）》
- (12) 《南方电网网络安全典型布防设计方案》
- (13) 《中国南方电网有限责任公司网络安全管理办法》

当规范与本技术规格书要求之间发生冲突时，采用其中最为严格的要求。本技术规范书中涉及的所有规范和标准均应采用现行最新版本，投标方采用的规范和标准不得低于所述规范和标准。若投标方发现本技术规范书与参照的文献之间有不一致之处应明确指出。投标方也可在投标文件中提出自己另外遵循的标准和规范，供招标方评价。

2. 项目概况

2.1. 项目目标

该项目采购标的为采购内容安全护栏，用于支持大模型应用识别、分类、应用评估、使用环境风险评估。

2.2. 项目范围

项目建设范围：广东电网有限责任公司广州供电局

项目建设单位：广州供电局数字运营中心

3. 项目工作内容

3.1. 项目内容

据广州供电局网络安全现状和需求，本项目开展内容安全护栏采购，用于支持大模型应用识别、分类、应用评估、使用环境风险评估。

具体如下

名称	基本功能配置要求	单位	数量	备注
2026 年网络安全技术防护-数字运营中心-内容安全护栏	1、提供一套内容安全护栏： ①基于流量检测，支持大模型应用识别、分类、应用评估、使用环境风险评估。支持对多种大模型应用外发途径识别和管控，进行文件格式和文件内容检测，支持大模型应用投喂内容进行敏感信息检测和过滤。支持对大模型应用外发文件进行病毒检测； ②提供含 5 年软件、协议库升级服务； 2、反向代理功能；3、大模型应用访问权限；4、大模型问答内容过滤；5、支持监测/阻断模式可以自由切换，支持允许和阻塞两种动作，可只检测不阻塞，也可检测风险时阻塞；可结合策略优先级及多策略的逻辑关系实现白名单、黑名单管控模式，并可设定例外或高优先级策略；6、SSL 加密解密；7、编码解码；8、实名授权问答；9、AI 问答敏感信息过滤；10、动态脱敏；12、AI 问答	套	1	技术要求详见 3.2

	记录；13、AI 问答业务监控；14、支持代答功能，可配置代答动作，设置代答对象。15、支持设定 AI 应用访问的并发连接数限制，以避免单用户大量访问对 AI 应用的压力，保障业务可用性；16、支持设定 AI 应用访问的速率限制；17、支持自定义脱敏规则；18、支持展示各敏感信息的占比；19、支持通过 DNS 代理解析策略；20、支持定义账号提取 AI 应用调用主体身份；21、支持模态相匹配的输入输出内容安全识别能力，具备文件真实类型检查及压缩加密等绕过方式拦截。22、支持结合业务特点，自定义复合脱敏规则，内容脱敏。23、支持重排脱敏。			
--	---	--	--	--

3.2. 技术要求

序号	章节	指标内容	优于判别条件	投标人提供值	符合情况
1	3.2	提示注入防护：支持对角色扮演注入、模拟对话注入、对立响应注入、反向诱导注入、分步骤诱导攻击等绕过模型原有过滤限制，诱导模型输出违法或不良信息的攻击行为进行检测与防护。	在满足指标内容的基础上，支持对 Base64、Unicode 等特殊编码内容解码检测，则该项为优于。		优于 / 满足 / 负 偏离
2	3.2	支持针对使用繁体中文绕过过滤等审核机制的注入手法进行检测。	在满足指标内容的基础上，支持针对使用英语语种绕过过滤等审核机制的注入手法进行检测。		优于 / 满足 / 负 偏离
3	3.2	内容合规性防护：支持对涉及政治敏感、违法犯罪等违反社会主义核心价值观内容，偏见、攻击性言论等歧视性内容，以及隐私泄露、侵权等侵犯他人合法权益内容进行检测和拦截。	/		满足 / 负 偏离

4	3.2	保密防护：支持对话料或知识库文件涉密内容进行扫描检测，支持对覆盖文本、文档等主流文件类型的输入输出涉密内容进行实时拦截，支持审计涉密操作行为。	在满足上述性能参数的基础上： 具备工信部软件与集成电路促进中心《大模型安全安全性检测证书》。		优于 / 满足 / 负 偏 离
5	3.2	性能参数： HTTP 每秒业务请求数量： 1000TPS 业务转发时延：≤20ms HTTPS 加密吞吐流量： 1Gbps 最大 HTTP 新建连接数： 1000 最大 HTTP 并发连接数：1 万	在满足上述性能参数的基础上： HTTP 每秒业务请求数量： 10000TPS 业务转发时延：≤5ms HTTPS 加密吞吐流量： 2.5Gbps 最大 HTTP 新建连接数： 3000 最大 HTTP 并发连接数：5 万。		优于 / 满足 / 负 偏 离
6	3.2	审计溯源： 对日志进行全量记录，包含访问时间、客户端 IP、URI、服务名称等基础信息、请求内容、请求 token 数量等请求信息、返回内容、响应 token 数量等返回信息、告警类型、响应动作等合规检测信息	在满足上述功能的基础上，还能支持根据会话 ID 等请求信息进行聊天内容上下文关联展示，支持按时间轴穿透查看历史上下文关联。		优于 / 满足 / 负 偏 离
7	3.2	动态脱敏： 支持对身份证号、手机号、银行卡号、姓名、地址、邮箱等个人敏感数据进行识别和脱敏。	/		满足 / 负 偏 离
8	3.2	敏感词识别： 支持自定义敏感词，支持基于敏感词对大模型输入输出内容进行检测。	/		满足 / 负 偏 离
9	3.2	内容检测策略： 支持白名单机制，用户可自定义配置大模型内容检测的白名单。	/		满足 / 负 偏 离
10	3.2	代码安全防护： 支持针对生成代码中潜在安全风险进行检测和预警，对恶意程序输出进行			满足 / 负 偏 离

		拦截。			
11	3.2	多模态内容防护： 支持针对图像、视频等多模态内容进行安全审核与风险拦截。			
12	3.2	内容分类与标签： 支持对检测到的违规内容进行自动化归类与分级管理。			满足/ 负 偏 离
13	3.2	MCP 防护： 支持对 MCP 消息内容进行安全检测，识别是否包含恶意指令、注入攻击或协议漏洞利用行为	在满足上述功能的基础上，还能支持对 MCP 上下文中的内容进行安全检测，识别并拦截包含恶意信息或敏感数据的上下文，防止上下文污染导致模型行为异常。		优于 / 满足 / 负 偏 离
14	3.2	动态防护策略： 支持配置不同场景下的防护强度切换条件，从而实现对多样化交互环境的自适应安全防护。	在满足上述功能的基础上，还能支持基于用户历史行为的画像构建规则，并可配置差异化防护策略的匹配与执行条件，从而实现对不同用户群体的精细化、个性化安全管控		优于 / 满足 / 负 偏 离
15	3.2	对抗样本防护： 支持针对产品自身对抗攻击的检测规则，并可配置绕过行为识别与反制策略，从而增强防护系统的抗攻击能力与鲁棒性。	/		满足/ 负 偏 离
16	3.2	软硬件使用许可永久授权；提供 5 年售后服务，含故障处理、漏洞修复、特征库升级等。	软硬件使用许可永久授权；提供 8 年售后服务，含故障处理、漏洞修复、特征库升级等。		优于 / 满足 / 负 偏 离

说明：投标商需对上述技术要求逐项应答，加“★”的关键技术点必须提供截图等必要证明方式，加盖公章；采购方保留在确定中标单位前，对投标人所投标的产品根据招标技术要求进行测试的权利，如果测试结果与投标人所投标书不符或弄虚作假者，将按有关规定取消其中标资格。

投标人应如实填写下表，汇总各关键参数及参数响应情况。

投标产品技术响应汇总表

名称	关键性能 参数数量	投标产品关键参数高 于 要求值	投标产品关键参数等 于要求值	投标产品关键参数低 于 要求值
		数量	数量	数量
2026 年网络安全技术防护-数字运营中心-内容安全护栏	/	/	/	/
物资名称	性能参 数数量	投标产品参数高 于要求 值	投标产品参数等 于要 求值	投标产品参数低 于要求 值
		数量	数量	数量
2026 年网络安全技术防护-数字运营中心-内容安全护栏				
物资名称	供货周期（承诺自签订合同起 XX 个工作日内完成物资的配送）			备注
2026 年网络安全技术防护-数字运营中心-内容安全护栏				

3.3. 项目转分包要求

1. 投标人不得将本合同项目转包给第三方。
2. 原则上不允许投标人将本合同项目分包给第三方，如确有需要，必须经招标人许可，投标人方可将本合同项目部分内容分包给第三方，且分包必须符合以下条件：
 - 2.1. 合同项目的主体部分不允许分包给第三方；
 - 2.2. 合同项目分包给第三方的比例不能超过或等于合同总额的 30%；
 - 2.3. 合同项目不允许分包给不符合相关资质要求的第三方；

- 2.4. 合同项目只允许一次性分包。
- 2.5. 套装软件或硬件产品的代理商合法代理行为，不应认定为转分包。

3.4. 项目验收与知识产权要求

1. 验收分为：到货验收（初步验收）、试运行合格验收（竣工验收）。
2. 中标方应向招标方提供有关本招标规范相关的全套技术文件。
3. 投标方应提供满足本技术规范书的相关技术资料。技术文档应全面、完整。
4. 招标方有权复制投标方提供的技术文件，作为设备的维护管理使用。
5. 本项目产生的文档、报告、程序以及过程中产生的脚本、工具等，其知识产权（包括软件著作权等）由招标人所有。
6. 招标人需就项目成果申请专利或者著作权备案的，投标人应予以协助。

3.5. 服务团队及服务能力

项目	项目角色	★基本人数要求	★基本资质要求
2026 年网络安全 技术防护-数字运 营中心-内容安全 护栏	项目经理	1 人。	项目实施团队经理具备 5 年以上信息安全维护经验，具有 PMP 或信息系统项目管理师认证。
	团队实施人员	2	具备信息系统建设实施经验。
	应急人员	3	熟悉信息系统建设实施经验，具备复杂故障处理能力。

1. 项目实施期间，投标方务必安排如下人员在具备以下技术条件的工作场地开展项目实施工作：
2. 场地开展项目实施工作：
3. 驻点人员驻点地点到招标方维护现场时间步行不得超过 10 分钟。
4. 工作场地具备网络、电话、指纹考勤设备、客户终端等设备，具有工作能力；场地、设备、网络接入等所需费用由投标方负责。
5. 工作电话能接入招标方 IT 服务中心 1000 电话系统，招标方服务台可将直接用户电话转接至项目参与人员工作电话。

-
6. 工作场地能接入招标方考勤系统，以便对维护人员进行考勤。
 7. 工作场地网络安装招标方指定的防病毒软件及安全技术策略。
 8. 实施期间驻场时间：按照广州供电局工作时间要求上班（8:00-12:00/14:00-18:00）。

3.6. 技术服务要求

3.6.1. 服务质量要求

中标方提供的技术服务支持服务应规范、及时、有效，准确，满足以下质量要求：

- 1) 保障技术服务支持期间资产管理系统运行稳定，不因为技术服务支持工作不规范、不及时、不到位或者工作失误，导致系统不可用时间超过 8.76 小时。
- 2) 保障技术服务支持期间系统运行安全，不因为技术服务支持工作不规范、不及时、不到位或者工作失误，发生三级及以上信息安全事件（信息安全事件分级定义见《广东电网有限责任公司安全生产风险分级管控和隐患排查治理双重预防机制管理实施细则》）。
- 3) 不因技术服务支持工作不规范、不及时、不到位或工作失误导致资产管理系统的系统数据、业务数据和配置信息丢失。
- 4) 不因技术服务支持工作不规范、不及时、不到位或工作失误以及工作态度问题导致用户服务满意度低于 90 分。
- 5) 严格遵循广东电网技术服务支持管理相关规定开展工作，杜绝技术服务支持工作违规事件，包括：遵守技术服务支持服务时限和服务周期规定，遵循技术服务支持流程规定，及时填写各种技术服务支持表单和记录，及时提交相关技术服务支持资料，按时参加各种技术服务支持工作会议。

3.6.2. 事件响应要求

事件响应流程必须满足广东电网有限责任公司广州供电局 IT 服务管理规范流程要求，具体事件响应要求如下，对系统严重问题消缺，中标人需承诺并提供证明，具备修改原代码的技术能力（本协议服务对象属于系统等级 2）：

事件影响度表

编号	影响度	说明
1	高	VIP 用户、所辖技术服务支持范围内二分之一及以上单位
2	中	所辖技术服务支持范围内二分之一以下单位
3	低	个别用户（1~3 人）

事件紧急度表

编号	紧急度	说明
1	紧急	信息安全事件、关键应用系统、关键信息基础设施故障、VIP 计算机终端故障
2	高	其他应用系统、信息基础设施故障
3	中	非 VIP 用户计算机终端故障
4	低	服务请求、硬件第三方维保等

事件优先级对应表

事件优先级对应		影响度		
		高	中	低
紧急度	紧急	紧急	高	中
	高	高	中	中
	中	中	中	低
	低	中	低	低

编号	分类	响应时间	到达现场时间	现场解决时间	根本原因分析	根本解决措施落实
1	紧急	5 分钟	45 分钟	2 小时	5 天	15 天
2	高	5 分钟	1 小时	4 小时	7 天	20 天
3	中	8 分钟	2 小时	8 小时	9 天	30 天
4	低	20 分钟	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求
5	一般	30 分钟	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求	按实际需要和广州局管理规定要求
6	其他	按实际需要和广州局管理规定要求				

注：

1、响应时间：对于紧急、高、中、低、一般等故障事件，中标人服务人员确保电话畅通，接收到报障通知并确认的时间。

-
- 2、到达现场时间：从响应时间开始算起；
 - 3、现场解决时间：从响应时间开始算起；
 - 4、根本原因分析：从响应时间开始算起；
 - 5、根本解决措施落实：从响应时间开始算起；
 - 6、严重问题：包括服务台接到多于三个部门或单位用户反馈的同一个系统使用问题、IT 集中监控系统监控到的重要及严重告警等。

3.7. 项目转分包要求

1. 投标人不得将本合同项目转包给第三方。
2. 原则上不允许投标人将本合同项目分包给第三方，如确有需要，必须经招标人许可，投标人方可将本合同项目部分内容分包给第三方，且分包必须符合以下条件：
 - 2.1 合同项目的主体部分不允许分包给第三方；
 - 2.2 合同项目分包给第三方的比例不能超过或等于合同总额的 30%；
 - 2.3 合同项目不允许分包给不符合相关资质要求的第三方；
 - 2.4 合同项目只允许一次性分包。

3.8. 网络安全管理要求

在为招标方提供软硬件产品或技术服务过程中，按照有关法律法规和程序开展工作，严格执行国家的有关方针、政策，并遵守以下规定：

（一）不利用招标方网络与信息系统从事危害国家安全、泄露国家秘密、侵犯公民、法人、招标方和其他组织的利益，或其它违法犯罪活动。

（二）不利用项目工作便利获取和留存招标方业务数据，不利用招标方业务数据谋取利益或从事其他与项目无关工作。

（三）交付的软硬件产品须满足招标方安全策略要求，不得含有后门、木马、已知漏洞等安全隐患。在其产品投运前，投标方应将产品有关的功能服务台帐、特权账号等建设运维文档全部移交给招标方。

（四）遵循招标方软件开发规范、安全合规要求开展系统开发部署及运行维护工作，配合招标方开展源代码审计工作。

（五）因投标方产品设计、开发缺陷造成其交付的产品在运行中出现安全隐患时，投标方应按招标方要求开展整改，并配合招标方开展其它支撑平台的安全整改。

（六）未经招标方许可，投标方不得将项目涉及的源代码、数据文件上传至互联网共享平台，或提供给其他组织和个人。

（七）投标方的开发测试环境中不得留存包含招标方企业名称、VI 标识、真实业务数据等信息。未经招标方许可，投标方不得在互联网上搭建与项目有关的测试、演示系统，确因工作需要开展测试演示的，测试环境中不得包含招标方企业名称、VI 标识、业务数据等信息，并在测试演示完成之后及时清理相关系统和数据。

（八）未通过招标方测试、备案的软件系统和设备不得私自上线运行。

（九）投标方在交付产品或服务质保期内，须根据《网络安全等级保护基本要求》、《南方电网公司网络安全合规库》以及招标方安全标准要求，完成安全加固配置、漏洞整改等工作。为招标方开展安全测试、安全加固等服务工作时，应及时清除服务过程产生的文件、服务、账号等信息，不得在招标方生产及测试环境留存病毒、木马文件及系统特权账号。

（十）投标方应对项目相关人员进行网络安全培训。项目实施人员上岗前须通过招标方组织的网络安全考试。

（十一）投标方项目实施人员应满足招标方对网络安全背景的审查要求。

（十二）投标方应落实网络安全责任，与招标方签订《网络安全协议书》（见附件）。

安全协议书应包含对投标方提出有关系统开发测试、数据保密、安全培训教育、配合提供软件源代码等相关责任义务。

3.9. 其他要求

1. 若因乙方违反信息安全相关法律法规、规章制度及文件规定，致使甲方存在重大信息安全隐患或发生信息安全事件的、造成甲方经济损失的，甲方有权扣除合同最终成交价 20%的违约金，违约金不足以弥补损失的，乙方还需赔偿实际损失。如经判定因乙方原因造成一般及以上信息安全事件（包括公司信息系统受损或形象受损），甲方有权扣除合同最终成交价 5%的违约金，违约金不足以弥补损失的，乙方还需赔偿实际损失。
2. 若乙方违反信息安全相关法律法规、规章制度及文件规定，甲方有权将乙方列入信息安全不良行为“黑名单”。一旦被列入“黑名单”，甲方有权立即终止与乙方的合同，且在 1 年内禁止乙方参与甲方的任何信息类业务。
3. 甲乙双方同意由于甲方原因引起的竣工时间延迟，通过函件或会议纪要的形式确认，不需要另行签订补充协议确认。
4. 相关税率按照国家有关政策或文件执行，含税价格按照税率变化进行相应调整。

4. 服务团队优异性表格

4.1. 一般服务团队条款/参数

应答范围：“3.5 服务团队及服务能力”章节，投标人必须如实填写一般服务团队条款/参数，如发现作假，则按照废标处理，其规格和内容如下：

序号	具体章节	指标内容	投标人提供值	符合情况
1	3.5	驻点人员驻点地点到招标方维护现场时间步行不得超过 10 分钟。		满足/ 负偏离
2	3.5	工作场地具备网络、电话、指纹考勤设备、客户终端等设备，具有工作能力；场地、设备、网络接入等所需费用由投标方负责。		满足/ 负偏离
3	3.5	工作电话能接入招标方 IT 服务中心 1000 电话系统，招标方服务台可将直接用户电话转接至项目参与人员工作电话。		满足/ 负偏离
4	3.5	工作场地能接入招标方考勤系统，以便对维护人员进行考勤。		满足/ 负偏离
5	3.5	工作场地网络安装招标方指定的防病毒软件及安全技术策略。		满足/ 负偏离
6	3.5	实施期间驻场时间：周一至周五，同甲方规定考勤时间。		满足/ 负偏离

注：

1. 投标人如实填写“投标人提供值”、“符合情况”；
2. “投标人提供值”：需列出所投产品/服务的具体内容，不得仅填写“满足”、“符合”等简单描述，同时未按照要求提供相关检测报告、截图、证明等，则该项判定为负偏离；
3. 符合情况：仅填入“满足”、“负偏离”。

4.2. 服务团队优异性表格

应答范围：“3.5 服务团队及服务能力”章节，投标人必须如实填写**服务团队优异性表格**中的**服务团队资质和服务能力**，如发现作假，则按照废标处理，其规格和内容如下：

序号	章节	指标基准要求	优于判别条件	投标人提供值	符合情况
1	3.5	★ 项目实施团队经理 1 人。 具备 5 年以上信息安全维护经验，具有 PMP 或信息系统项目管理师认证。	1、具有 CISSP、CISP、OCM、OCP、DM7-DCA 证书、ITIL、OCS 资质之四。		满足/ 负偏离
2			在满足指标基准要求的情况下，满足以下条件，则该项为优于。 1、具有 10 年以上工作经验。		满足/ 负偏离
3	3.5	★ 团队实施人员 2 人。 具备信息系统建设实施经验。	在满足指标基准要求的情况下，满足以下条件，则该项为优于。 1、提供本地化技术服务能力。		满足/ 负偏离
4			在满足指标基准要求的情况下，满足以下条件，则该项为优于。		满足/ 负偏离

			1、大于 4 人的支撑团队。		
5			在满足指标基准要求的情况下，满足以下条件，则该项为优于。 1、至少 2 人具备 CCIE/H3CIE/HCIE/CISSP 其中之一认证；		满足/ 负偏离
6			在满足指标基准要求的情况下，满足以下条件，则该项为优于。 1、至少 2 人具备信息网络安全专业技术人员资质。		满足/ 负偏离
7	3.5	★ 应急人员 3 人。 熟悉信息系统建设实施，具备复杂故障处理能力。	在满足指标基准要求的情况下，满足以下条件，则该项为优于。 1、人员具备 CCIE/H3CIE/HCIE/CISSP 其中之一认证。		满足/ 负偏离

注：

1. 投标人如实填写“投标人提供值”、“符合情况”；
2. “投标人提供值”：需列出所投产品具体参数值，不得仅填写“满足”、“符合”等简单描述，同时未按照要求提供相关检测报告、截图、证明等，则该项判定为负偏离；
3. 符合情况：填入“优于”、“满足”、“负偏离”，如优于判别条件为该项无优于，则填入“满足”。

5. 技术条款/技术参数点对点应答表

投标人必须如实填写技术条款/技术参数点对点应答表中的一般条款/参数，如发现作假，则按照废标处理，其规格和 content 如下：

序号	具体章节	指标内容	投标人提供值	符合情况
1	1.4.1	投标人应标时，必须向招标人提供拟派参加本项目的人员名单以及参加人员的资料，如甲方要求，现场人员需在合同签订后一周内安排招标人面试或考试。		满足/ 负 偏 离
2	1.4.1	投标人必须向招标人保证工程人员组织的稳定性，必须向招标人提供拟派参加本项目的人员名单以及参加人员的资料，在本项目工程结束前，现场实施人员与投标人应标不一致的，参加本项目的人员变动必须取得招标人同意，且在投标文件承诺变动人员的资质必须等同或高于实施人员的资质，每次变动需出具人员入场证明，增补人员的资质需提供等同或高于实施人员的资质证明文件并取得招标方同意。		满足/ 负 偏 离
3	1.4.2	投标人应保证所提供的实施服务满足本技术规范书各项要求。		满足/ 负 偏 离
4	3.2	产品完全满足密评、信创要求。 承诺可通过 SNMP 配置、API 接口配置和 SYSLOG 配置等方式将性能、日志等数据提供至 ITSCADA 系统统一纳管及监控。 承诺可开放接口与我局现有软硬件平台对接。		满足/ 负 偏 离
5	3.1	针对甲方环境和重要保障需求，分析网络和布防情况，定制化大屏，实时展示布防有效性。		满足/ 负 偏 离

6	其他一般技术条款/技术参数	其他所有一般技术条款/技术参数（不包含本表格已列出的一般技术条款/技术参数） 注：如不能满足要求，需详细列明差异性，否则，招标人即认为投标人可以满足本技术规范书的要求）		满足/负偏离
---	---------------	---	--	--------

注：

1. 投标人如实填写“投标人提供值”、“符合情况”；
2. “投标人提供值”：需列出所投产品/服务的具体内容，不得仅填写“满足”、“符合”等简单描述，同时未按照要求提供相关检测报告、截图、证明等，则该项判定为负偏离；
3. 符合情况：仅填入“满足”、“负偏离”

6. 主要条款/参数优异性表格

投标人必须如实填写主要条款/参数优异性表格中的主要条款/参数优异性，如发现作假，则按照废标处理，其规格和内容如下：

序号	章节	指标内容	优于判别条件	投标人提供值	符合情况
1	3.2	针对繁体中文注入手法进行检测。繁体中文是指使用繁体绕过关键字过滤等审核机制，然后再让模型翻译输出违法或不良信息	针对英语语种注入手法进行检测。英语语种是指使用英语绕过关键字过滤等审核机制，然后再让模型翻译输出违法或不良信息		满足/负偏离
2	3.2	性能参数： HTTP 每秒业务请求数量：1000TPS 业务转发时延：≤20ms HTTPS 加密吞吐流量：1Gbps 最大 HTTP 新建连接数：1000 最大 HTTP 并发连接数：1万	在满足上述性能参数的基础上： HTTP 每秒业务请求数量：10000TPS 业务转发时延：≤5ms HTTPS 加密吞吐流量：2.5Gbps 最大 HTTP 新建连接数：3000 最大 HTTP 并发连接数：5万		满足/负偏离

3	3.2	<p>审计溯源：</p> <p>对日志进行全量记录，包含基础信息（访问时间、客户端 IP、URI、服务名称等）、请求信息（请求内容、请求 token 数量等）、返回信息（返回内容、响应 token 数量、响应延迟等）、合规信息（合规评分、告警类型、响应动作）</p>	<p>在满足上述功能的基础上，还能支持根据会话 ID 进行聊天内容上下文关联展示，支持按时间轴穿透查看历史上下文关联</p>		满足/负偏离
4	3.2	<p>身份认证鉴权：</p> <p>支持自动提取并关联前端访问大模型的真实用户名，实现用户身份与大模型访问行为的精准关联</p>	<p>在满足上述功能的基础上，还能支持支持基于提取的真实用户名做访问控制和动态脱敏。</p>		满足/负偏离
5	3.2	<p>动态脱敏：</p> <p>内置敏感数据识别标签，支持身份证号、手机号、银行卡号、姓名、地址、邮箱等个人敏感数据识别。</p>	<p>在满足上述功能的基础上，还能支持对识别的敏感数据配置拦截和动态脱敏等处理动作，从而实现敏感数据的精确控制，预防敏感数据泄露。</p>		满足/负偏离
6	3.2	<p>敏感词识别：</p> <p>支持违规内容拦截，采用关键字匹配、语义相似度分析、AI 辅助识别三重技术，对“提问、推理、回答”进行内容检测。可有效拦截涉黄、涉恐、涉爆等违规内容，帮助客户审查大模型输入输出内容，保障信息输入输出遵守法律法规</p>	<p>在满足上述功能的基础上，还能支持用户自定义敏感词，满足不同行业和场景的个性化需求</p>		满足/负偏离
7	3.2	<p>提示词安全防护：</p> <p>配置实时拦截与深度研判相结合的防护策略，包括意图解析模型的调用规则，从而实现对越狱攻击、注入攻击等恶意输入的精准识别与多层次处置</p>	<p>在满足上述功能的基础上，还能支持对提示词进行深度语义分析，理解用户真实意图，判断是否存在隐藏的恶意目标或越狱企图。</p>		满足/负偏离
8	3.2	<p>代码安全防护：</p> <p>支持针对代码弱风险用法的检测规则，并可配置不</p>	<p>在满足上述功能的基础上，还能支持代码风险分类规则，并可配置风险等</p>		满足/负偏离

		安全的加密、权限提升、数据泄露等安全隐患的识别策略，从而实现对生成代码中潜在安全风险的全局扫描与预警	级判定条件与结构化输出模板，从而实现对检测到的代码风险进行分级归类与信息标准化输出。		离
9	3.2	多模态内容防护： 支持针对图像内容的检测规则，并可配置不当、有害及敏感内容的识别策略，从而实现对输入与生成图像的自动化安全审核与风险拦截。	在满足上述功能的基础上，还能支持视频内容检测规则，并可配置帧级或整体分析策略，从而实现对视频中不当、有害及敏感内容的精准识别与拦截。		
10	3.2	推理时安全引导： 支持基于 SafeSteer 的安全策略动态调整规则，并可配置针对特定输入类别的干预机制，从而实现在推理过程中的低延迟、精准化安全干预	在满足上述功能的基础上，还能支持自动干预决策规则，并可配置多级干预策略（如拒绝、改写、告警等）的触发条件与执行动作，从而实现对检测结果的动态响应与分级处置。		满足/ 负 偏 离
11	3.2	内容分类与标签： 支持违规内容分类规则，并可配置暴力、色情、政治敏感、仇恨言论等类别的判定策略，从而实现对检测到的违规内容进行自动化归类与分级管理	在满足上述功能的基础上，还能支持内容风险等级标记规则，并可配置高危、中危、低危及信息等级别的判定条件，从而实现对检测内容的分级标识与差异化处理		满足/ 负 偏 离
12	3.2	RAG 防护： 支持对意图判定规则进行配置与调整，对用户检索查询内容进行解析，识别是否存在获取敏感信息或绕过访问控制等隐藏恶意目标，并基于配置结果对查询请求进行拦截或告警处置	在满足上述功能的基础上，还能支持对授权知识库来源清单进行配置与维护，对检索结果来源进行追踪与校验，识别并标记来自恶意或未授权来源的结果		满足/ 负 偏 离
13	3.2	MCP 防护： 支持通过 MCP 消息内容安全检测规则，对 MCP 消息内容进行安全检测，识别是否包含恶意指令、注入攻击或协议漏洞利用行为	在满足上述功能的基础上，还能支持通过 MCP 上下文安全检测规则，对 MCP 上下文中的内容进行安全检测，识别并拦截包含恶意信息或敏感数据的上下文，防止上下文		满足/ 负 偏 离

			污染导致模型行为异常。		
14	3.2	A2A 防护： 支持通过 Agent 通信安全端到端加密策略，对 Agent 间通信进行端到端加密，防止通信内容被窃听或泄露。	在满足上述功能的基础上，还能支持通过 Agent 调用链路完整性校验规则，对 Agent 调用链路中的各个环节进行完整性检查，确保链路中每一步操作均为合法行为		满足/ 负 偏 离
15	3.2	动态防护策略： 支持基于对话上下文的动态防护策略则，可配置不同场景下的防护强度切换条件，从而实现对多样化交互环境的自适应安全防护。	在满足上述功能的基础上，还能支持基于用户历史行为的画像构建规则，并可配置差异化防护策略的匹配与执行条件，从而实现对不同用户群体的精细化、个性化安全管控		满足/ 负 偏 离
16	3.2	软硬件使用许可永久授权；提供 5 年售后服务，含故障处理、漏洞修复、特征库升级等。	软硬件使用许可永久授权；提供 8 年售后服务，含故障处理、漏洞修复、特征库升级等。		满足/ 负 偏 离

7. 优选总体方案定义

项目	优选总体方案（项目概况）
2026 年网络安全技术防护-数字运营中心-内容安全护栏	投标方产品方案思路清晰，产品方案合理，项目实施内容及进度描述详细，具有可操作性，管理体系完善，内容详细，可操作性强，突出特点；方案需充分考虑与现有平台的集成，实现本质安全建设的目的。

8. 质量保证及售后服务要求

8.1. 售后服务总要求

1、在系统投入运行后，在质保期内投标方如对其系统软件有所改进，均应为招标方提供最新版本免费使用。

2、在相关的应用系统进行调试或升级时，中标方有责任派技术人员到现场完成相关工作。

8.2. 技术维护支持服务

技术支持人员在质保期内应随时待命协助用户方人员维护系统。技术支持服务应满足下列要求：

- 1、技术支持的范围涵盖系统中所有与本项目相关的软硬件；
- 2、提供广州本地化技术服务团队；
- 3、紧急技术支持应能提供 7x24 小时服务；
- 4、应根据解决问题所需的专门技术，派遣专人处理紧急事件；
- 5、提供的技术维护服务不得免除本应承担的质量保证责任；
- 6、验收（终验）后提供 5 年免费维保，包括特征库升级，投标方不得以功能授权为由限制产品的功能使用。
- 7、质保期由完成项目终验之日起开始计算，质保费用已经在投标文件的报价部分报价，并计入总价范围。质保期内，乙方须保证每月至少一次安全巡检，及时处理当期出现的系统问题，保证在质保期内进行免费升级。
- 8、投标方在质保期内须保证的技术支持服务：
 - 提供 7*24 小时远程技术支持服务以及必要的护网期间现场技术支持服务。
 - 及时处理系统软件故障。
 - 及时消除系统软件设计和实施上的缺陷。
 - 如果所采购设备在保修期内出现重大故障，投标方应在接到招标方通知后 2 小时内作出响应并尽快提供解决方案。如果必须由投标方进行现场故障处理才能恢复系统正常的，投标方须立即派遣项目技术人员用最快捷的交通工具前往现场，并在 8 小时内恢复系统正常。在解决问题后，投标方应以书面方式详细说明导致故障的原由及解决问题时所采取的措施。
- 9、无论是否在质保期内，投标方所提供的系统升级服务均不应造成系统功能缺陷和性能下降。
- 10、投标方应给出质保期内的具体系统维护、升级和技术服务等的内容和方案。

8.3. 技术支持人员要求

中标方必须组建技术支持团队，负责在质保期内对招标范围项目的安全技术保障和服务响应支持。团队要求如下：

1、中标方必须提交质保期内技术支持服务流程图；

2、团队必须设置总体负责人，总体负责人专门负责质保期内所有技术支持的协调工作、中标方与招标方的所有正式联络等工作；

3、中标方应提交团队人员名单和相关资料，所有人员必须经招标方选择和认可。如无特殊原因并未经招标方许可，该人员名单在合同执行过程中不允许更改。

9. 项目创新评价专项标准

本项目用以下标准评价交付物创新水平：

项目创新评价指标						
指标 维度	一级 指标	二级指标	评价内容	得分（每项）		
创新 价值	技术 价值	协助完成重大科技攻关	国家科技重大专项	36		
			国家重点研发计划、“科技创新-2030”重大项目、国务院国资委关键核心技术攻关项目	27		
			国家自然科学基金集项目	18		
			省部级科技计划项目、国家自然科学基金（不含集成项目）	12		
			南方电网公司重大科技专项或南方电网公司基础前瞻专项项目	9		
			南方电网公司科技项目（网级决策项目）	6		
			南方电网公司科技项目（分子公司决策项目）	3		
	行业	成果协同获得价	评价内容	一等	二等	三等

价值	价值	值创造奖励	南方电网公司价值创造奖	6	4	2.5
			分子公司成果价值创造奖	2	0.9	0.3
		成果协同获得专利奖励	项目	金奖	银奖	优秀奖
			中国专利奖	30	22	15
			省专利奖	10	7	5
		成果协同获得技术标准奖励	项目	一等	二等	三等
			中国标准创新贡献奖	20	15	9
			行业级标准创新贡献奖	14	10	6
			南网公司技术标准贡献奖	7	5	3

创新能力	专业能力	协助在国际组织、行业组织专业性任职	等级	负责人、主任委员、秘书长、副主任委员、副秘书长、会士	秘书、委员、理事、顾问	
			国际级	50	20	
			国家级	30	14	
			行业级	20	8	
			省行业级	10	4	
		协助入选人才支持计划	等级	第一档	第二档	第三档
			国家级	50	45	40
			省部级	30	25	20
			地市政府级	10	8	3
			南网公司级	10	8	3
			分子公司级	5	3.5	2
			地市企业级	3	2	1
		协助获得人才荣誉或奖励	等级	第一档	第二档	第三档
			国家级	20	15	10
			省部级/行业级	10	8	5
			地市政府级	5	3.5	2
			南网公司级	5	3.5	2

			分子公司级	3	2	1
			地市企业级	1	0.8	0.5
		支撑竞赛获奖	项目	一等	二等	三等
			国家级竞赛获奖	12	10	7
			国家部委级/行业级竞赛 获奖	10	7	5
			省级竞赛获奖	7	5	3
			南网公司级竞赛获奖	6	4	2
			分子公司级竞赛获奖	3	2	1
	支撑学术技术成果影响力	等级	主旨发言	一般发言/论文宣读		
			国际级	12	4	
			国家级	6	2	
			省部级/行业级	3	1	
		支撑主持或主要编制技术标准	等级	我局主编	核心起草人员 (前 30%)	一般人员
			国际标准	20	10	5
			国家标准	10	7	3.5
			行业标准、地方标准	6	4	2
			团体标准	3	2	1
			企业标准	3	2	1
		支撑规范编制 (制度规范、技术手册、业务指导书、规划、意见)	等级	我局主编	核心起草人员 (前 30%)	一般人员
			行业级	5	3	1.5
			南网公司级	3	2	1
			分子公司级	1	0.5	0.25
			地市企业级	0.5	0.25	0.125
		支撑获得专利权	等级	获得授权	实质审查	
			国际专利	5 分/项	2 分/项	

			发明专利	2 分/项	1 分/项	
			实用新型专利（包含软件著作权）	0.5 分/项	0.2 分/项	
			外观设计专利	0.2 分/项	0.1 分/项	
		支撑发表论文	等级	我局第一作者	我局普通作者	
			发表 SCI 收录论文	6 分/项	2.5 分/项	
			发表/EI 收录论文	5 分/项	2 分/项	
			在中国科学引文数据库（CSCD）收录期刊、北大核心期刊发表 1 篇论文	2 分/项	1 分/项	
			在科技核心期刊发表 1 篇论文	1.5 分/项	0.5 分/项	
			专业期刊发表文	0.5 分/项	0.2 分/项	
	支撑成果转化		评价细分	我局人员排名 第 1	排名第 7 以内	排名第 15 以内
			纳入国家能源领域首台（套）重大技术装备目录	25	19	11
			纳入中央企业科技创新成果推荐目录	23	29	37
			纳入工信部“一条龙”中央企业应用示范目录	20	14	6
			纳入南方电网新技术推广应用目录	18	12	4
			纳入南方电网公司技术试运行目录	15	9	1
	人才 发展 贡献	支撑教材及题库编制、课件开发、岗位评价标准编制、参与专家选	等级	组长	核心起草人员 （前 30%）	一般人员
			行业级及以上	6	4	2.5
			南网公司级	4	3	1

		聘或考核评审等	分子公司级	2	1	0.5
		任务	地市企业级	1	0.5	0.25
		支撑知识培训授课	等级	1个月及以上	1周及以上至1个月以下	1周以内
			行业级及以上	6/项	4/项	2.5/项
			南网公司级	4/项	3/项	1/项
			分子公司级	2/项	1/项	0.5/项
			地市企业级	1/项	0.5/项	0.25/项
社会影响	社会评价	支撑相关工作获得社会荣誉	等级	第一档	第二档	第三档
			支撑相关工作获得以下奖项的： 国家级别奖项、 广东省科学技术厅广东省科学技术奖	30	20	15
			支撑相关工作获得以下奖项的： 全国性行业级别奖项、 省级奖项	15	10	7
			支撑相关工作获得以下奖项的： 全国性一般组织级别奖项 (非行业主要组织) 省行业级别奖项、 市级奖项	8	5	3

备注：用于评价各类项目对我局创新工作支撑情况，以对我局相关事项做出较大技术支撑为准。

计算规则：不同事项可累加，如不同课题获得同一奖项；同一事项取最大值，如同一论文取最前作者；同一项适用不同评价项时取分值较高项。

10. 违约责任

合同终止条款：

若出现以下情况之一的，招标人有权终止合同并追究相关法律责任。

1、合同履行期间内，累计出现一次一级安全事件。

2、合同履行期间内，累计出现两次二级安全事件。

3、合同履行期间内，累计出现三次三级安全事件。

4、招标人有权对中标人项目参与人员进行面试或者考试（面试或者考试范围为项目工作内容），发现驻场人员资质或工作经验造假情况。

5、中标人项目参与人员未经招标人书面同意而参加其他项目工作，或未经招标人书面同意更换项目参与人员数量超过总数比例20%。

6、经招标人发出部门整改通知书3次或以上，或广州局整改通知书2次或以上。

11. 效力说明

本技术规范书作为招标方案的附件，与招标方案具有同等法律效力。

（以下无正文）