



2025 年网络安全技术防护(网络安全软硬件 采购)项目(日志审计系统(日志分析与管 理系统计算节点))技术条件书

深圳供电局有限公司

2025 年 7 月

目 录

1 工作范围	3
1.1 供货范围	3
1.2 服务界限	4
1.3 服务期限	4
2 引用标准	4
3 技术要求	5
3.1 日志分析计算节点（日志分析与管理系统计算节点）（3 个）	5
4 资料管理	7
4.1 文档范围	7
4.2 投标方的责任	7
4.3 随机手册	7
4.4 文档种类	7
4.5 其它	7
5 售后服务及技术培训	7
6 质量保证	9
7 试验与调试	10
7.1 验收要求	10
7.2 测试报告	10
7.3 现场调试和现场试验（SAT）	11
7.3.1 现场调试	11
7.3.2 现场试验	11
8 技术性能偏差表	11
9 投标方需说明的其他问题	11

总则

1.1 本技术条件书适用于深圳供电局有限公司 2025 年网络安全技术防护（网络安全软硬件采购）项目采购，以及相关设备的功能、性能、安装等方面的技术要求。

1.2 本技术条件书提出的是最低限度的技术要求，并未对一切技术细节做出规定，也未充分引述有关标准和规范的条文，投标方应提供符合本技术条件书和工业标准的优质产品。

1.3 如果投标方没有以书面形式对本技术条件书的条文提出异议，则意味着投标方提供的设备(或系统)完全符合本技术条件书的要求。如有异议，不管是多么微小，都应在报价书中以“对招标技术文件的意见和同招标技术文件的差异”为标题的专门章节中加以详细描述。

1.4 本技术条件书所使用的标准如遇与投标方所执行的标准不一致时，按较高标准执行。

1.5 本技术条件书经招、投标双方确认后作为订货合同的技术附件，与合同正文具有同等法律效力。

1.6 投标方在应标技术文件中应如实反映应标产品与本技术条件书的技术差异。如果投标方没有提出技术差异，而在执行合同的过程中，招标方发现投标方提供的产品与其应标技术文件的条文存在差异，招标方有权利要求退货，并将对下一年度的评标工作有不同程度的影响。

1.7 投标方应在应标技术部分按本技术条件书的要求如实详细的填写应标设备的标准配置表，并在应标商务部分按此标准配置进行报价，如发现二者有矛盾之处，将对评标工作有不同程度的影响。

1.8 投标方应充分理解本技术条件书并按本技术条件书的具体条款、格式要求填写应标的技术文件，如发现应标的技术文件条款、格式不符合本技术条件书的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.9 本技术条件书未尽事宜，由招、投标双方协商确定。

1 工作范围

1.1 供货范围

本技术条件书要求采购的深圳供电局有限公司 2025 年网络安全技术防护（网络安全软硬件采购）项目采购供货范围包括：

设备名称	数量
日志审计系统（日志分析与管理系统计算节点）	3 个

1.2 服务界限

从生产厂家至招标投标方应选派有经验的技术人员，对安装和运行人员免费培训方指定交货点的运输和装卸全部由投标方完成；

现场安装和试验在投标方的技术指导和监督下由招标方完成，投标方协助招标方按标准检查安装质量，处理调试投运过程中出现的问题。

1.3 服务期限

自合同生效之日起至 2026 年 6 月 30 日。

2 引用标准

除本招标书另有说明外，投标方提供的所有设备均应按照下列标准进行设计、制造、检验和安装。所用的标准必须是最新版本。如果这些标准的内容有不同之处时，应按照最高标准的条款执行或按双方协商同意的标准执行。如果投标方选用本条件书以外的标准时，需提交这种替换标准相当于或优于本条件书规定的标准的说明。标准如下：

- (1) ISO-----国际标准化组织标准
- (2) IEC-----国际电工委员会标准
- (3) ITU-T----国际电信联盟标准
- (4) IEEE-----美国电气电子工程师协会标准
- (5) EIA-----电子工业协会标准
- (6) GB-----中华人民共和国国家标准
- (7) DL-----中华人民共和国电力行业标准
- (8) 《电力二次系统安全防护规定》
- (9) CCITT -----国际电报和电话咨询委员会
- (10) ITU-----国际电信联盟。
- (11) UL-----美国保险商试验室标准。
- (12) NFPA -----美国国家防火协会标准。
- (13) SI-----标准国际单位制。
- (14) NEMA-----美国国家电气制造协会标准。
- (15) ANSI
- (16) 其它招标方指定的规约

3 技术要求

其中★项目为关键参数。▲项目为重点评分项，如优于指标要求需提供证明材料并加盖公章。

1、★本项目采购的设备须满足自主可控要求，满足 IPv4/IPv6 协议双栈要求，提供承诺函。

2、★产品到货后按照国家及南网的要求，如需开展系统入网安评、商用密码应用安全性评估、信息系统安全等级测评及备案等合规性审查工作，以及如需开展数认平台、统一密码平台等安全管控系统接入集成工作，涉及相关系统集成及网络安全测评费用且无其他相关项目支撑的，由投标方承担所投产品的集成与测评费用，提供承诺函。

3、★采购设备在并网投运时应确保不存在弱口令风险，在维保期内发现弱口令风险应按合同和技术协议要求整改，提供承诺函。

4、参数指标

3.1 日志审计系统（日志分析与管理系统计算节点）（3 个）

指标项	指标子项	指标要求
硬件规格	硬件要求	▲至少具备 2 个 CPU，每个 CPU≥（16 核心 32 线程，主频 2.5GHz）、内存≥256G（总容量）DDR4；硬盘 1：2 块 960G SSD 固态硬盘组成 Raid 1；硬盘 2：不小于 12*4TB 企业级 SATA 3.5 寸硬盘；电源：冗余双电源；网口：4 个千兆电口、2 个万兆光口（含两个 SFP+多模光模块）
数据采集与存储	数据采集	支持对网络设备、安全设备、主机系统的日志、网络流量等多种数据源的采集； ▲支持接入并管理日志采集器、流量采集器，可支持第三方采集器接入（提供功能截图证明） 支持对日志采集器进行采集配置并下发；提供 Syslog、SNMP Trap、文本格式日志、数据库、WMI、Netflow、HTTP、Script 等采集方式；并支持数据源信息导入、导出、数据源迁移操作。
	数据存储	支持新增日志类型功能，可在线新增字段信息，支持数据存储类型的配置，包括：ES、Kingbase、mysql，支持存储基础信息的配置：包括数据库名、存储时间、分区方式等基础属性信息，从而达到分类存储日志的目的
资产管理和风险评估	资产管理	支持主机资产管理功能，资产分类至少包括服务器、工作主机、网络设备、安全设备、终端安全管理、数据库、中间件、存储设备、应用服务器、虚拟化设备等类型，支持对 IPV6 资产的管理。
		支持资产详情信息的展示，能够展现资产名称、IP 地址、分组、厂商、型号、操作系统、物理地址、责任人、是否外连情况等资产基础信息。
		支持从资产分组、组织架构、业务分组、地理位置及网段视角展示主机资产详情信息。
		支持资产服务信息管理，支持对服务的 IP 地址、端口号、

		服务名、服务版本、协议、Banner 等服务属性进行管理。
	资产发现	支持通过网络流量被动发现资产信息、支持通过脆弱性发现资产信息，资产信息至少包含：IP 地址、服务、服务版本、协议、端口、操作系统、主机名、mac 等。
响应处置	自动更新 SOC 工单数据	自动编排处置后，更新 SOC 的工单操作记录及工单状态。
	SOC 跟自动编排单点登录	通过 SOC 可以单点登录到自动编排平台，无需输入账号密码。
告警数据	告警数据自动发送给自动编排	通过关联规则配置告警产生，并自动创建工单，同时发送告警数据到自动编排系统
	告警数据手工发送给自动编排	发现告警后，先派工单到责任人，责任人分析研判后，下发告警数据到自动编排系统
态势大屏	态势首页	提供态势感知大屏统一入口，态势首页集中展示至少 10 块态势大屏；支持大屏配置、轮播投放，内置大屏介绍文档，可供用户线上查看和下载；
		支持对态势大屏的内网地理位置、重点关注区域进行修改；支持自定义大屏 LOGO；支持设置大屏启停、轮播间隔时间、大屏轮播顺序
		态势大屏数量不少于 10 个，维度不限于综合安全态势、安全运营态势、威胁预警态势、外部威胁态势、内网威胁态势、攻击者态势、资产态势、资产风险态势、全网脆弱性态势、告警实时监控大屏
统计报表	报表管理	支持快速报表、周期报表功能、自定义模板三种方式 自定义报表模板：支持自定义模板可加入多种统计分析视图（含自定义）和智能备注信息（可根据数据不同展示不同的备注说明）；支持灵活编辑和布局调整以形成整体报表；可添加不限于告警统计、工单统计、异常行为统计、弱口令统计、攻击者统计、日志统计、系统维护、脆弱性统计、调查统计、资产统计、风险统计等；报表模板可被快速报表和周期报表任务引用
	统计视图	统计视图支持不限于：列表、指标卡，折线图、面积图、堆积面积图、柱状图、堆积柱状图、条形图、堆积条形图、饼图、玫瑰图、散点图、词云图、双轴图等视图展示。
系统管理	升级管理	支持统一系统软件版本、威胁情报、漏洞知识库、IP 地址定位库、巡检规则包、威胁预警包等数据的升级，支持配置升级地址并展示当前版本和升级相关信息，支持手动/自动升级方式
	角色管理	支持用户角色管理，可以为不同角色赋予不同系统功能模块及数据的读写权限（提供功能截图证明）
	安全性	支持系统账户的安全性验证，包含双因子认证、账户登录设置、可信主机等设置，支持对登录异常账户锁定、密码长度、密码强度、登录会话并发数等进行设置；支持配置可信主机；开启双因子认证，认证方式支持短信、邮件、企业微信、企业钉钉、蓝信。（提供功能截图证明）
	知识库	支持知识库管理，内置漏洞知识库、IP 地址定位知识库、ATT&CK 知识库、应用识别知识库、事件日志 ID 知识库。 支持自定义知识库，支持对自定义知识库字段的管理和配置，字段包含文本框、富文本、数值、密码、附件等表现形式，支持自定义知识库的增删改查等基础配置。
仪表盘	自定义仪表	支持自定义仪表盘功能，能够在仪表盘内加入多种统计分

	板	析视图（含自定义），支持在引用视图时查看视图内容，还支持跳转到视图模块新增视图便于仪表板快速引用。支持选择、拖拽、边框调整等操作，形成账户独有的仪表板展示页面。（提供功能截图证明）
--	---	--

4 资料管理

4.1 文档范围

- 1) 投标方提供的文档包括系统技术资料、维护手册、培训资料、和用户手册等。
- 2) 提供的文档还应包括由投标方采购供货的第三方设备的软件的技术手册及相关资料。

4.2 投标方的责任

投标方应对其所提供的全部文档的准确性和完整性负责。所有由投标方采购供货的第三方设备的技术手册的准确性由投标方负责。

4.3 随机手册

对每一设备都应有完整的、装订好的安装图和说明手册，随设备装箱一起运至现场。

4.4 文档种类

投标方必须至少提供以下文档（所有文档提供电子文档一份）：

项目	说明	数量
1	用户使用手册	1
2	系统维护手册	1
3	系统功能说明手册	1
4	系统安装和配置手册	1
5	系统测试手册	1

4.5 其它

在投标方定购设备到货后，投标方应立即准备以下文档各 1 份交给招标方：

- 1) 全部订购系统的型号、技术特点和性能参数清单。
- 2) 所有主要部件和连接线缆的材料规格。

5 售后服务及技术培训

5.1 软件类系统技术服务要求

- 1) 提供 3 年的原厂安全和性能补丁服务；
- 2) 提供 1 年原厂标准服务，包含：

- 提供 7×24 小时技术支持服务，指定相对固定的技术负责人及联系电话、传真、e-mail 等。
- 在用户发现软件缺陷时，投标方必须在用户提出维护要求的 2 小时内作出响应，24 小时内提交故障分析报告和解决方案，48 小时内故障得以解决。
- 重大软件故障时，投标方应在接到故障电话后 4 小时到达现场，24 小时内修复故障。
- 在有新的系统补丁或升级版本时，在征得用户同意的情况下可进行升级或打补丁。由于未提供给用户补丁或升级而引起的运行故障由投标方负责一切后果。

5.2 硬件类系统技术服务要求

1) 提供 3 年的设备保修服务；

2) 提供 1 年原厂标准服务，包含：

- 提供 7×24 小时技术支持服务，指定相对固定的技术负责人及联系电话、传真、e-mail 等。
- 在用户发现系统缺陷时，投标方必须在用户提出维护要求的 2 小时内作出响应，24 小时内提交故障分析报告和解决方案，48 小时内故障得以解决。
- 重大系统故障时，投标方应在接到故障电话后 4 小时到达现场，24 小时内修复故障。
- 在有新的系统补丁或升级版本时，在征得用户同意的情况下可进行升级或打补丁。由于未提供给用户补丁或升级而引起的运行故障由投标方负责一切后果。

5.3 技术培训

- 1) 投标方应由资深系统研发专家为招标方的技术人员开设现场培训课程。招标方的技术人员应在安全防护设备的部署、运行维护等各方面得到培训，熟悉和掌握运行、检查、修理和维护相关安全防护设备并掌握软件开发工具。
- 2) 投标方应向受训人员提供技术资料、图纸、参考材料、培训手册等；还应提供测试设备、工具和安全设备，以及其它必需品和工作场地。
- 3) 投标方应提出对受训者最为有利的培训计划(包括培训时间、地点、内容)。
- 4) 投标方应向招标方提交培训时间表和课程表，投标方应定出培训大纲，培训

大纲和计划应提交招标方确认，根据招标方实际运行需求进行修改。

5) 免费提供培训，甲方选派人员参加；培训内容为相关系统的现场安装、调试、维护、使用、故障诊断等；

5.4 中标人须为合同产品提供硬件 3 年、软件 1 年原厂技术支持和服务和软件 3 年安全及性能补丁更新服务，投标时须提供原厂服务承诺函。

5.5 在系统频繁出现故障、或遇重大节假日等特殊情况下，需要提高系统维护等级的情况下，应招标人要求，应提供技术人员提供现场技术支持，及时处理各类故障。

5.6 一旦发现系统运行不稳定，而与合同产品有关，须免费提供合乎原厂商规定的合同产品的更新或版本升级，或对系统进行维修、维护，直至问题得到解决。

5.7 免费进行必要的软件更新和版本升级。当招标人准备对合同产品进行升级或扩容时，须提供咨询服务，并提交相关方案。

5.8 向招标人提供合同产品相关的新技术的日常技术咨询服务。

5.9 系统发生搬迁时，中标人须派遣专业技术人员现场支持，免费提供合理、可行的搬迁技术方案给招标人并保证搬迁后系统的正常运行。

5.10 提供免费实施，投标方所投标价格中需要包含系统的安装部署。

5.11 提供免费开发，投标方提供与招标方的自动化运维平台、态势感知系统的接口开发与对接，不在单独收取任何费用。

6 质量保证

6.1 订购的新型产品除应满足本规范书外，投标方还应提供产品的鉴定证书。

6.2 投标方应保证制造过程中的所有工艺、材料等（包括投标方的外购件在内）均应符合本规范书的规定。若招标方根据运行经验指定投标方提供某种外购零部件，投标方应积极配合。

6.3 投标方应遵守本规范书中各条款和工作项目的 ISO9000、GB/T1900 质量保证体系，该质量保证体系已经过国家认证和正常运转。

6.4 质保期间，因制造质量问题而发生损坏，或不能正常工作时，投标方应免费为招标方修理或更换零部件（质保期按设备投运日算起一年或投标方的最后一种设备到货之日算起一年半，两者以先到日期为准）

7 试验与调试

7.1 验收要求

1) 本项目仅进行现场验收（SAT）。且为针对整个项目的验收，不单独对本设备进行验收测试，但投标方应配合系统集成商进行整个项目的验收测试，并负责设备的验收测试相关资料的编制及其它配合性工作。

2) SAT 验收测试大纲根据项目招标技术文件、投标技术应答书、合同技术协议书等技术文件的内容编写，由投标方编制，招标方审核批准。

3) 投标方应在验收测试前 2 周提供详细的 SAT 验收测试大纲，大纲应提供所有现场验收的细则，细则指定的实验项目以及达到的性能指标不得小于本招标文件要求。招标方有权提出一些合理的特殊测试，并保留对大纲的修改权力。大纲经双方确认生效后，招标方人员对验收的认可签字并不解除投标方对合同的保证责任。

4) 投标方将负责对现场安装和测试进行指导，投标方的工程师将协助进行现场试验验收。

5) 在现场验收完成后 20 天内，双方的代表将签署验收报告。

6) 验收计划由投标方准备，交给招标方审查同意。

7) 为有利于系统的安装、投运和测试，投标方应派出有经验的专家提供技术服务。

8) 在现场安装、投运及验收过程中，投标方应对损坏的设备负责。

9) 备品备件、文档资料均作为验收的一部分。

7.2 测试报告

在 SAT 测试完成后的二十天内，投标方应提供四份测试报告的副本，每份报告至少包括以下内容：

1) 设备说明。

2) 报告编号、日期。

3) 设备的项目编号、数量及顺序号。

4) 测试的时间、地点及方法。

5) 测试环境。

6) 试验数据包括表计型号、读数、测试点的位置、数据打印出的结果及有关图形等。

7) 测试合格的标准。

8) 测试人员名单。

9) 负责人签字。

7.3 现场调试和现场试验（SAT）

7.3.1 现场调试

- 1) 设备运到现场安装完毕, 招标方应通知投标方人员到场参加设备调试。
- 2) 在调试过程中, 若发现设备存在元器件损坏或不正常工作情况, 投标方应负责更换。

7.3.2 现场试验

- 1) 现场验收应在所有设备安装调试完毕, 且设备准备投入试运行进行, 并出具书面测试报告。
- 2) 现场验收应在工厂系统试验完全完成的基础上进行。
- 3) 在验收开始前二周相应的安装调试单位应提出 SAT 验收大纲供招标方认可, 投标方予以配合。

8 技术性能偏差表

投标方应将所供设备与本招标书技术文件有差异之处, 无论优于或劣于本招标书技术文件要求, 均汇集至以下表中。

技术差异表

序号	采购技术条件书		投标文件	
	条目	简要内容	条目	简要内容

9 投标方需说明的其他问题

如有需说明的其他问题, 投标方应通过书面形式提交, 并加盖公章。