



# 日志审计系统技术规范书

深圳供电局有限公司

2026 年 01 月

# 目 录

1 总则 .....	1
2 工作范围 .....	1
2.1 项目概况 .....	1
2.2 范围和界限 .....	2
2.3 服务范围 .....	2
3 应遵循的主要标准 .....	3
4 使用环境要求 .....	4
5 技术要求 .....	5
5.1 设备技术要求 .....	5
5.2 设备技术参数和性能要求响应表 .....	5
5.3 设备及其附件主要元器件来源 .....	7
6 试验 .....	8
6.1 型式试验 .....	8
6.2 出厂试验 .....	8
6.3 现场交接试验和功能验收 .....	8
7 产品对环境的影响 .....	8
8 技术文件要求 .....	8
9 监造、包装、运输、安装及质量保证 .....	9
9.1 监造 .....	9
9.2 包装 .....	9
9.3 运输 .....	9
9.4 质量保证 .....	9
10 技术差异表 .....	10
11 投标方需说明的其他问题 .....	10

## 1 总则

1.1 本技术规范书适用于深圳供电局有限公司\_\_\_\_\_项目采购的日志审计系统,它提出了该设备本体及附属设备的功能设计、结构、性能、安装和试验等方面的技术要求。

1.2 本设备技术规范书提出的是最低限度的技术要求。凡本技术规范书中未规定,但在相关设备的行业标准、国家标准或 IEC 标准中有规定的规范条文,投标方应按相应标准的条文进行设备设计、制造、试验。对国家有关安全、环保等强制性标准,必须满足其要求。

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

1.4 本技术规范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 本技术规范书经招标、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的法律效力。若本技术规范书涉及有关商务方面内容,如与招标文件的商务部分矛盾时,以商务部分为准。

1.6 本技术规范书未尽事宜,由招标、投标双方协商确定。

1.7 投标方在应标技术规范书中应如实反映应标产品与本技术规范书的技术差异。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规范书的条文存在差异,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。

1.8 投标方应在应标技术部分按本技术规范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。

1.9 投标方应充分理解本技术规范书并按本技术规范书的具体条款、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、格式不符合本技术规范书的要求,则认为应标不严肃,在评标时将有不同程度的扣分。

1.10 标注“★”的条款为关键条款和技术参数,作为评标时的否决项。

## 2 工作范围

### 2.1 项目概况

本技术规范书采购的设备适用的工程概况见表 2.1：工程概况一览表。

表 2.1 工程概况一览表 （项目单位填写）

序号	名 称	内 容
1	采购设备或项目名称	
2	项目单位	深圳供电局有限公司
3	项目单位地址	深圳市福田区中心一路 39 号

## 2.2 范围和界限

1) 本技术规范书适用于所供设备的设计、制造、装配、工厂试验、交付和试验的指导、监督以及试运行工作。

2) 本技术规范书未说明，但又与设计、制造、装配、试验、运输、包装、保管和运行维护有关的技术要求，按条款 3 所规定的有关标准执行。

## 2.3 服务范围

### 1) 供货范围一览表

投标方提供的设备及其附件的具体规格、数量见表 2.2：设备供货范围响应表。投标方应如实填写“投标方保证”栏。

表 2.2 设备供货范围响应表（项目单位填写）

序号	名 称	单位	项目要求		投标方保证	
			型式、规格	数量	型式、规格	数量
1	日志审计系统	套	按设备技术参数和性能要求响应表响应	1		

2) 投标方所提供的组件或附件如需向第三方外购时，投标方应对其质量向招标方负责，并提供相应出厂和验收报告。

3) 投标方应协助招标方解决设备运行中出现的问题。

4) 如果调试、性能试验、试运行及质保期内技术指标一项或多项不能满足合同技术部分要求，买卖双方共同分析原因，分清责任，如属制造方面的原因，或涉及索赔部分，按商务部分有关条款执行。

5) 设备正常使用后，投标方和招标方（业主）双方应根据相关法律、法规和公司管理制度签署合同设备的验收证明书。该证明书共两份，双方各执一份。

6) 投标方应按招标方要求免费提供必须的人员培训和技术指导，确保招标方正常使用和维护设备。

### 3 应遵循的主要标准

除本技术规范书特殊规定外，投标方所提供的设备均按规定的标准和规程的最新版本进行设计、制造、试验。如果这些标准内容有矛盾时，应按最高标准的条款执行或按双方商定的标准执行。如果投标方选用本技术规范书规定以外的标准时，则需提交这种替换标准供审查和分析。仅在投标方已证明替换标准相当或优于技术规范书规定的标准，并从招标方处获得书面的认可才能使用。提交供审查的标准应为中文或英文版本。标准如下：

ISO	《国际标准化组织标准》
IEC	《国际电工委员会标准》
ITU—T G. 652、G. 655	《单模光纤标准》
IEEE	《美国电气电子工程师协会标准》
GA 1089-2013	《电力设施治安风险等级和安全防范要求》
DL	《中华人民共和国电力行业标准》

EIA	《电子工业协会标准》
	《中华人民共和国网络安全法》
GB 50348-2018	《中华人民共和国密码法》
GB17859-1999	《计算机信息系统 安全保护等级划分准则》
GB/T25058-2019	《信息安全技术 网络安全等级保护实施指南》
GB/T25070-2019	《信息安全技术 网络安全等级保护安全设计技术要求》
GB/T 22240-2020	《信息安全技术 网络安全等级保护定级指南》
GB/T22239-2019	《信息安全技术 网络安全等级保护基本要求》
GB/T28448-2019	《信息安全技术 网络安全等级保护测评要求》
DL/T 860	《变电站通信网络和系统》
	《电力二次系统安全防护规定》
Q/CSG 115001-2012	《南方电网调度自动化系统不间断电源配置规范》
	《南方电网公司反事故措施（2018 版）》
电监信息[2012]62 号	电力行业信息系统安全等级保护基本要求

#### 4 使用环境要求

本设备招技术规范书技术文件需要采购的设备，其外部使用条件见下表。投标方应对所提供的设备性能参数在外部条件下进行校验、核对，使所供设备满足实际外部条件要求及全工况运行要求。

设备使用环境要求相应表（项目单位填写）

序号	名 称	项目要求值	投标方保证值	备注
1	长期工作环境温度	10℃～35℃		
2	存储温度	0℃～55℃		
3	长期工作环境相对湿度	35%～80%		
4	存储相对湿度	10%～95%		
5	长期工作海拔高度	0m～1000m		
6	存储海拔高度	0m～1000m		

## 5 技术要求

### 5.1 设备技术要求

#### 5.1.1 设备基本要求

设备及全部配件必须为全新的、持久耐用的产品。即使在本技术规范书中没有明确地提出,也应满足作为一个完整产品一般所能满足的全部要求。同时,可根据系统、测试对象性能的要求并随着 IT 技术发展,可提供持续的软件开发和硬件的升级。

#### 5.1.2 设备结构要求

无要求。

### 5.2 设备技术参数和性能要求响应表

投标方应认真逐项填写所供设备技术参数和性能要求响应表 5.2.1-5.2.3 中“投标方保证值”栏,不能空格,也不能以“响应”两字代替,不允许改动本表内“投标方保证值”栏之外的数值。如有差异,请填写表 10.1: 技术差异表。标注“★”的条款为关键条款,投标方应出具相应技术资料证明达到条款和技术参数的要求,作为评标时的否决项。

#### 5.2.1 日志审计系统

指标	类别	技术要求说明
产品要求	硬件要求	★2U 标准机架式设备,提供冗余电源;CPU≥8,内存≥128,系统盘≥128G SSD,数据盘≥4*16T 硬盘,接口≥4*千兆电,≥4*千兆光,≥2*万兆光口,2*USB,1*串口,1*GE 管理口,1*扩展插槽,具备液晶显示屏。
	★安全要求	产品集成部件的芯片基于自主可控芯片,包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
	性能要求	系统支持审计≥540 台日志源设备接入,应可扩展日志源接入数量。系统支持≥13000EPS/秒的日志平均处理能力
	系统架构	系统应基于大数据平台架构,具备海量数据收集与快速检索能力
		系统应基于 B/S 架构,支持 SSL 加密模式访问,可通过 web 方式直接对系统进行管理
	日志采集	★系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等(需要提供加盖制造商公章的功能截图)
		系统支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap 等方式采集日志 ★系统应支持规则自适应日志接入,仅输入端口即可自动匹配相应规则,完成日志自动接入,(需要提供加盖制造商公章的功能截图和具有 CMA 或 CNAS 认证的第三方权威检测机构出具的检测证明)

		系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、奇安信、亚信、艾科网信、Windows、Linux/Unix、、HUAWEI(华为)、H3C(华三)、Apache、nginx、IIS、WebLogic、Vmware、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等
		★系统支持利用 JDBC 的方式对数据库表日志进行综合管理与分析，（需要提供加盖制造商公章的功能截图和具有 CMA 或 CNAS 认证的第三方权威检测机构出具的检测证明）
		系统支持采集国产化数据库数据接入，包括但不限于：人大金仓、南大通用、达梦数据库，神州通用
	日志管理	★系统支持采集国产化操作系统日志，包括但不限于：中标麒麟、银河麒麟、统信、openEuler 等，（需要提供加盖制造商公章的功能截图）
		★系统应支持综合态势大屏概览，直观展示系统运行天数、日志保存天数、日志总数、各日志类型日志数量、当日事件统计 TOP5、CPU/内存/磁盘等系统资源占用情况，并能够可视化展示日志源设备活跃情况、日志接入速率趋势图、近 7 日日志量趋势图、近 7 日事件量趋势图，便于运维人员及时发现日志接入异常，（需要提供加盖制造商公章的功能截图）
		系统应能实现海量日志数据的采集并保存原始日志数据
		系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据
		★系统应支持界面配置即可完成未识别日志接入，无需编写 xml。（需要提供加盖制造商公章的功能截图）
		★系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译，（需要提供加盖制造商公章的功能截图）
		★系统应内置对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联等，（需要提供加盖制造商公章的功能截图和具有 CMA 或 CNAS 认证的第三方权威检测机构出具的检测证明）
		★系统应内置对 WEB 服务器日志展开深度分析，分析内容包括但不限于发起请求的地址及浏览器情况、响应结果、访问趋势等，（需要提供加盖制造商公章的功能截图）
		系统应支持 IPv4、IPv6 日志数据的采集、范式化、分析、展示
		★系统应支持对资产进行监控配置，包含资源监控、采集监控、采集限速等，（需要提供加盖制造商公章的功能截图和具有 CMA 或 CNAS 认证的第三方权威检测机构出具的检测证明）
	日志转发	系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息
	日志备份恢复	系统应支持按类型、按日期(天)，手动、自动备份日志
		系统应支持设置日志存储备份策略，可设置备份周期、备份日志类型



		★系统应支持将产生硬件故障但能 WEB 访问设备上的数据备机到新设备上，备机数据应包含日志源、事件规则、统计项、枚举值等，（需要提供加盖制造商公章的功能截图和具有 CMA 或 CNAS 认证的第三方权威检测机构出具的检测证明）
	日志查询分析	系统应支持实时日志查询、历史日志查询，实时日志查询支持 3 分钟、5 分钟、10 分钟、30 分钟不同频次刷新频率 系统应支持从日志属性或资产属性对日志进行检索，日志属性可自定义添加字段为检索条件，资产属性可基于资产标签进行二次检索 系统应支持全量日志查询，无需加载冷数据
	事件告警	系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别 ★系统应支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式。（需要提供加盖制造商公章的功能截图）
	资产管理	系统应支持资产属性配置 ★系统应支持资产监控，支持根据设备类别对资产进行分类，根据 IP 可下钻至资产的整体数据、告警及关联事件。（需要提供加盖制造商公章的功能截图）
	报表管理	★系统应能够按照多种维度统计日志信息，包括但不限于攻击日志、审计过滤、恶意程序、防火墙、主机报表、应用服务器、网络设备、Windows 审计、Linux 审计、终端审计、SOX 合规、PCI 合规、ISO 27001 合规等多种场景。（需要提供加盖制造商公章的功能截图）
	用户管理	★系统应该支持国密 (SM) 多因子认证登录能力，并可指定用户。（需要提供加盖制造商公章的功能截图）
	系统部署	系统应支持 IPv4、IPv6 部署
资质	产品资质	★产品需具有《网络安全专用产品安全检测证书》或《网络关键设备和网络安全专用产品安全认证证书》，提供证书复印件证明并加盖制造商公章 ★中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，级别至少为 EAL3+，提供证书复印件证明并加盖制造商公章 国家版权局颁发的《计算机软件著作权登记证书》，提供证书复印件证明并加盖制造商公章

### 5.3 设备及其附件主要元器件来源

投标方应按下表如实填写主要元器件来源。

设备及附件主要元器件来源一览表 （投标方填写）

序号	元器件名称	型号	厂家或供应商名称	产地	备注

--	--	--	--	--	--

## 6 试验

根据相关国标和行标等有关标准及其补充说明进行各项试验,有关条款的特殊要求和补充应在试验期间遵守并执行。

### 6.1 型式试验

型式试验是为了验证所设计和制造的设备的性能是否能够达到相应产品标准的要求,投标方应提供有相应资质的第三方检测机构出具的产品型式试验报告,型式试验的项目内容如下:

无

### 6.2 出厂试验

出厂试验是为了发现产品所用材料和制造中的缺陷,它不应损伤产品的性能和可靠性。出厂试验应在整体组装后进行,应该对每台成品进行检验,以确保每台产品与已经通过型式试验的产品相一致。出厂试验的项目内容如下:

无

### 6.3 现场交接试验和功能验收

本技术规范书采购设备应进行现场交接试验和功能验收。交接试验和功能验收是为了确认设备经过运输、储存和/或调整等过程后是否存在损坏、各个单元的兼容性、装配是否正确。

## 7 产品对环境的影响

投标方应该提供有关设备对环境影响所需要的材料。任何已知的化学危险和环境危害应在手册或使用说明中明确。

投标方应该对有关设备的不同材料的使用寿命和拆除的程序给予必要的指导,对再循环使用的可能性给予简要说明。

## 8 技术文件要求

在设备到货时,投标方应按招标方要求提供满足本次采购设备、调试、使用、维护所需要的相关技术文件纸质版至少 2 套,电子版资料 1 套。投标方提供的所有资料均应 为中文版或中英文对照版。投标方提供本次采购设备所需的软件应为原装正版软件。具体要求提供资料如下:

- a. 出厂试验报告;

- b. 产品合格证；
- c. 产品安装说明书和产品使用手册（包括：软件和硬件安装使用说明、系统功能说明、调试方法、维护项目、培训教程等等）。
- d. 其它相关图纸资料、测试数据、软件密钥等等；

## 9 监造、包装、运输、安装及质量保证

### 9.1 监造

本技术规范书采购设备无监造要求。

### 9.2 包装

1) 要严格按照制造厂给出的说明书对设备进行包装、运输和储存。制造厂应在交货前的适当时间提供设备的运输和储存说明书。

2) 设备制造完成并通过试验后应及时包装， 否则应得到切实的保护。其包装也应符合铁路、公路和海运部门的有关规定。

3) 包装箱上应有明显的包装储运图示标志， 并应标明招标方的订货号和发货号。

4) 设备的包装应能保证设备各零部件在运输过程中不致遭到脏污、损坏、变形、丢失及受潮。对于其中的绝缘部件及由有机绝缘材料制成的绝缘件应特别加以保护，以免损坏和受潮。对于外露的接触表面，应有预防腐蚀的措施。所有运输措施均应经过验证。凡有运输损坏，应由制造厂负责赔偿。

### 9.3 运输

1) 设备单独运输的零部件应有标志，便于用户安装装配。

2) 整体产品或分别运输的部件，都要适合于运输及装卸的要求。

3) 制造厂应提供按全部解体检修用的备品备件和装用机具，随同产品发运。

4) 随同运输的产品应附有装箱清单，产品所需提供的技术资料应完整无缺。

### 9.4 质量保证

1) 全部设备必须是全新的， 持久耐用的，应满足作为一个完整产品所能满足的全部要求。投标方应保证设备在规定的使用条件下运行、预期使用寿命应不少于 12 年。

2) 投标方应对其整组设备在到货后提供不少于 3 年的“三包”质量保证。之后如发生产品损坏，投标方应及时为本组装置提供维修部件，并按最近的投标价提供。

3) 订购的新型产品除应满足本标准外，投标方还应提供该产品的鉴定证书。

4) 投标方应保证制造过程中的所有工艺、材料试验等（包括投标方的外购件在内）均应符合本标准的规定。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。

5) 附属及配套设备必须满足有关行业标准的要求，并提供试验报告和产品合格证。

6) 投标方应有遵守本标准中各条款和工作项目的 ISO9000-GB/T19000 质量保证体系，该质量保证体系已经通过国家认证并在正常运转。

7) 对仪器设备在质保期内出现的故障，投标方人员在接到通知后应在 2 个工作日内派技术人员到现场检查处理，并立刻提出处理意见，免费进行维修。

8) 对于质保期已过的仪器设备，厂家将负责终身维修。对于一般的故障，处理时间 15 个工作日内。对于严重的故障，将根据情况安排维修时间的长短。

## 10 技术差异表

投标方应将所供设备与本招技术规范书技术文件有差异之处，无论优于或劣于本招技术规范书技术文件要求，均汇集至表 10.1。

表 10.1 技术差异表 （投标方填写）

序号	招 标 文 件		投 标 文 件	
	条 目	简 要 内 容	条 目	简 要 内 容

## 11 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。