|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 附件1 | | | | | | | | |
| 小额采购项目报价书 | | | | | | | | |
| 一、采购项目名称：广州市志愿者行动指导中心2022-2023年信息系统运行维护项目 | | | | | | | | |
| 二、询价单位名称：广州市志愿者行动指导中心 | | | | | | | | |
| 三、询价单位联系人： 联系电话： | | | | | | | | |
| 四、报价单位名称：\*\*\*公司 | | | | | | | | |
| 五、报价单位联系人： 联系电话： | | | | | | | | |
| 六、本次报价有效期：从 年 月 日至 年 月 日，共 天。 | | | | | | | | |
| 七、分项报价清单如下： | | | | | | | | |
| 序号 | 采购项目内容 | 规格要求 | 数量 | 单价 | 金额（元） | 预计完成时间 | 备注 | |
| 1 | “志愿时”系统运维服务 |  |  |  |  |  |  | |
| 2 | 基础支撑系统运维服务 |  |  |  |  |  |  | |
| 3 | 桌面运维服务 |  |  |  |  |  |  | |
| 4 | 网络安全服务 |  |  |  |  |  |  | |
|  | 合计 |  |  |  |  | 大写： | | |
| 附件：1.报价单位营业执照复印（盖章） | | | | | | | | |
| 2.填写《采购需求清单》（盖章） | | | | | | | | |
| 报价单位名称（加盖公章） | | | | | | | | |
| 报价时间： 年 月 日 | | | | | | | | |
|  | | | | | | | |

附件2

采购需求清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 预算：人民币56.78万元 | | | | | |
| 资格要求： | | | | | |
| 1 | 符合《政府采购法》第二十二条供应商资格条件；分公司报价的，必须由具有法人资格的总公司授权。 | | | | |
| 采购范围 | | | | | |
| 1 | 采购内容 | | | 项目名称：广州市志愿者行动指导中心2022-2023年信息系统运行维护服务项目  本期项目信息系统运维服务的具体内容及模式如下：  1.信息系统运维服务  (1)志愿时系统运维服务  (2)基础支撑系统运维服务  2.桌面运维服务  3.网络安全服务 | |
| 项目工期要求 | | | | | |
| ☑从合同签订之日起 12 个月。 | | | | | |
| 项目背景 | | | | | |
| 我中心自身近年来进行了一定规模的信息化建设，采购了日常使用的IT设备及重要的业务应用系统，目前网络和信息安全设备24台，视频监控设备1套，网络综合信息点100个，应用系统2套等。随着我中心对整体IT系统（硬件、软件、网络通讯）的可用性要求日益提高，系统运行保障和维护管理就成为确保业务系统安全稳定可靠运行的最有力的手段。这些设备的日常保养、故障网络集成和检测维护、系统维护等的工作量巨大，而我中心目前的信息化建设实施、网络维护等工作由于人力有限，建设任务繁重，较难做到IT设备及业务系统的日常维护服务的高效和保质保量，为了保障我中心信息化设备、软件系统的安全稳定运行，出现故障时能在最短时间得以恢复，保证业务工作的正常开展，迫切需要专业的IT服务公司对当前建有的应用系统以及硬件设施提供定期保养、故障维修、运行维护以及安全检查服务，以避免出现各类问题造成对工作的冲击和影响，减少因IT设备故障和系统故障造成的影响带来的损失，提高我中心办公区域内的软、硬件、业务应用软件的运行维护效率，确保信息系统正常运行。 | | | | | |
| 运维目标需求 | | | | | |
| （一）提高IT设备的使用效率，合理的设备维护提高设备使用时间，降低设备维修成本，提升办公效率的和节约办公经费；  （二）工作效率的提升，使得办公人员能够更高效地完成工作任务；  （三）专业的外包服务给信息化化建设提供数据决策，合理使用办公经费；  （四）改进的速度和服务获取专门技能。  本项目有计划地解决了信息系统的维护问题，全面提高我中心人员办公质量，建立良好的办公环境。 | | | | | |
| 运维服务的范围 | | | | | |
| ☑基础设施维护 | | | | | □服务器与相关设备维护  □办公自动化设备维护  ☑网络和信息安全设备维护  ☑视频监控、防盗报警设备维护 |
| ☑软件及信息资源维护 | | | | | ☑业务系统维护  □工具软件维护 |
| □链路租赁和云平台租赁迁移服务 | | | | | □链路租赁  □虚拟机服务器租赁服务 |
| ☑其他运维服务 | | | | | ☑信息安全服务  ☑等保测评服务 |
| 运维服务工作要求 | | | | | |
| **一、信息化现状**  我中心自身近年来进行了一定规模的信息化建设，采购了日常使用的IT设备及重要的业务应用系统，目前网络和信息安全设备24台，视频监控设备1套，网络综合信息点100个，应用系统2套等。随着我中心对整体IT系统（硬件、软件、网络通讯）的可用性要求日益提高，系统运行保障和维护管理就成为确保业务系统安全稳定可靠运行的最有力的手段。这些设备的日常保养、故障网络集成和检测维护、系统维护等的工作量巨大，而我中心目前的信息化建设实施、网络维护等工作由于人力有限，建设任务繁重，较难做到IT设备及业务系统的日常维护服务的高效和保质保量，为了保障我中心信息化设备、软件系统的安全稳定运行，出现故障时能在最短时间得以恢复，保证业务工作的正常开展，迫切需要专业的IT服务公司对当前建有的应用系统以及硬件设施提供定期保养、故障维修、运行维护以及安全检查服务，以避免出现各类问题造成对工作的冲击和影响，减少因IT设备故障和系统故障造成的影响带来的损失，提高我中心办公区域内的软、硬件、业务应用软件的运行维护效率，确保信息系统正常运行。  **1.1基础设施现状**   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **序号** | **设备名称** | **设备型号** | | **数量** | **购置时间** | **到保时间** | | 一、网络设备 | | | | | | | | 1 | 交换机 | D-Link DES-1024A | | 3 | 2011/11/18 | 2012/11/17 | | 2 | 核心交换机 | 华三S3100 | | 1 | 2010/11/18 | 2011/11/17 | | 3 | 路由器 | 艾泰 Hiper2000 | | 1 | 2011/11/18 | 2012/11/17 | | 4 | 接入交换机 | D-Link DES-1016A | | 4 | 2011/11/18 | 2012/11/17 | | 5 | 网络OPE交换机 |  | | 1 | 2019/4/28 | 2020/4/27 | | 6 | 流控路由 | IK-G10 | | 1 | 2019/4/28 | 2020/4/27 | | 7 | 24口POE交换机 | RG-NBS1826GC-LP | | 1 | 2019/4/28 | 2020/4/27 | | 8 | 交换机 | LS-5120V2-28P-HPWR-LI | | 1 | 2019/4/28 | 2020/4/27 | | 9 | 路由器 | ER8300G2 | | 1 | 2019/4/28 | 2020/4/27 | | 10 | 无线AP | IK-X3 | | 9 | 2019/4/28 | 2020/4/27 | | 11 | 小计 |  |  | 23 |  |  | | 二、信息安全设备 | | | | | | | | 1 | 防火墙 | 深信服AF-12020 | | 1 | 2020/11/10 | 2017/11/9 | | 2 | 小计 |  | | 1 |  |  | | 三、其他设备 | | | | | | | | 1 | 信息点 | AMP | | 100 | 2010/4/16 | 2013/4/13 |   **1.2.软件及信息资源现状**   |  |  |  |  | | --- | --- | --- | --- | | **序号** | **系统名称** | **系统正式运行时间** | **备注** | | | 1 | 志愿时 | 2010/11/1 |  | | 2 | 志愿服务志交会交会网站 | 2012/10/10 |  |   **二、运维服务内容**  **2.1信息系统运维服务**  本期信息系统运维服务的具体内容：  （一）基础设施维护，包括定期巡检、系统故障监测与排除、备件服务、版本升级与补丁更新等服务。  （二）软件及信息资源维护，包括定期巡检、系统故障监测与排除、应急响应等。  （三）其他内容与服务  1.项目管理服务。  2.IT运维管理体系咨询服务。  **2.1.1志愿时系统**  **2.1.1.1志愿时运维服务**  “志愿时”系统是团广州市委、亚组委志愿者部在亚运期间开发的志愿者管理系统，广泛应用于志愿者招募、录用、培训、排岗、考勤、维系、激励等领域，实现了对59万名亚运志愿者的信息化、流程化、标准化管理，极大提升了亚运志愿服务工作的组织运行水平。亚运后，团广州市委联合广州市科信局、民政局在亚运“志愿时”系统基础上，融合“智慧城市”的发展理念，进一步深化并提升成为“志愿时”综合管理系统。“志愿时”综合管理系统不仅是常态化、全流程、在线式志愿服务综合管理平台，更是一套加强提升包括志愿服务组织在内的社会组织能力建设的信息化、智能化、规范化软件工具。  2011年，升级了“志愿时”系统（社区版1.5系统）。从行政化组织与社会化动员相结合的角度，对“志愿时”系统从基本概念和基础模型上进行优化，实现了“两个转变”，即由大型赛会志愿者管理向常态化志愿服务管理转变；由单一时间管理平台向志愿服务“三要素”（志愿者、志愿服务组织、服务项目）综合规范化管理平台转变。  2013年，升级打造了“志愿时”系统2.0版本，增加了互动社交功能，优化了用户体验，奠定了“智慧志愿”的建设理念、概念和产品设计架构、技术雏形和发展方向，培养线上交易、线下服务的专业运营团队和服务意识，以最优化的配置来保障系统的日常运行，更好、更快地为广大志愿者、志愿组织服务。作为全国首个志愿服务智慧云平台，集成志愿者、组织和服务项目的交互交流和管理功能，是广州共青团在志愿服务领域进行的成功尝试，成为服务广东全省各地市志愿服务的最权威的品牌，具有很大的社会影响力。  2014年，打造升级了“志愿时”系统3.0版。用互联网思维实现志愿服务全生态开放、扁平化运行，通过对接线上线下的社会网络，让志愿服务渗入人们的生产消费、工作生活、婚恋交友等方方面面，进一步丰富志愿者的公益社交圈子生活。  2019年，“志愿时”系统4.0版将根据中央文明办、民政部和共青团中央组织有关单位制定的《志愿服务信息系统基本规范》(MZ/T 061-2015)，按照据广州市“数字政府”建设和管理工作的相关要求，结合广州市志愿服务工作业务需求建设。“志愿时”系统4.0版主要聚焦推进运用5G、大数据、人工智能等信息化新技术，向青年志愿者提供个性化、精准化、主动化服务的管理系统。务求使志愿服务组织、青年志愿者以“志愿时”系统为运行中枢，以协同运作，优化工作流程、精简办事材料，实现审批更简、监管更强、服务更优的系统为建设原则，以建设市区联通、部门协同、规则一致、标准统一、一网通办的“互联网+志愿服务”体系为目标的志愿服务综合管理系统。  “志愿时”管理系统：加强对志愿者工作时间“志愿时”的量化管理，并激励广大志愿者对社会贡献自己的力量；从而进一步加强了对志愿者工作的信息化管理。  “志愿时”管理系统 截至2020年5月，在系统中，广州市实名注册志愿者为313万人，累计志愿服务时长58952761.45小时。  广州市志愿者行动指导中心系统运行维护服务项目以IT运维管理为基础，以外包IT服务为核心，以报警和事件为手段，加强IT全局的管理，提高IT服务的响应时间，降低IT管理和服务的成本消耗，依托第三方专业IT服务商的技术力量建立起标准、规范的IT运维与服务管理平台。IT运维与服务管理平台将以往对网络、服务器与业务应用、安全设备、客户端PC等的分割管理进行了有效的整合，利用拓扑技术，实现全面监控与集中统一管理；并融入了基于ITIL理念的IT服务流程管理，实现了技术、功能、服务三方面的有机结合，同时，整合了第三方专业的IT服务商的服务支持，从而提高了广州市志愿者行动指导中心IT系统的运行管理水平和服务能力（原由团市委立项开发的志愿时评测管理系统，因志愿者相关业务已转移给指导中心，故将系统划拔给指导中心运营和维护）。  **2.1.1.1.1 软件应用系统运行情况表**   |  |  |  | | --- | --- | --- | | 序号 | 指标名称 | 运行情况 | | 1 | 年度业务量（件） | 3,381,750 | | 2 | 年度新增数据量（条） | 8,454,375 | | 3 | 活跃用户数（个） | 1,690,875 | | 4 | 正常运行率（%） | 100% | | 5 | 故障及时响应率（%） | 100% | | 6 | 是否部署在政务云 | 是 | | 7 | 软件首次投入运行时入库资产金额（万元） | 279 |   **2.1.1.1.2 是否部署云系统**  是部署在云系统。  **2.1.1.1.3 软件运维需求表**   |  |  |  |  | | --- | --- | --- | --- | | 序号 | 类型 | 服务内容 | 维护要求 | | 1 | 日常维护 | 系统性能日常维护 | 1.工作内容：（含系统运行状态监控及预警）：定期巡检（周期：每周一次）； 负责资产及版本管理、定期补丁升级、日志检查分析、错误分析及统计，系统修复；  2.巡检周期：每周一次 | | 2 | 系统故障检测及排除 | 响应时间及排除故障时间：不影响业务正常开展的故障，在工作日内4个小时内解决；影响到业务正常开展的故障，在工作日内2个小时内解决。 | | 3 | 驻场要求 | 1.驻场  2.驻场人员数量：1名  3.服务时间：8\*5  支持系统日常运营活动审核和维护等。 | | 4 | | 5 | 系统优化 | 补丁及接口升级 | 对系统进行补丁及接口升级 | | 6 | 性能优化 | 主要包括应用消息队列、共享内存优化；应用服务能力优化，例如应用进程数、应用线程数的优化；应用日志级别及日志空间的调整； |   **系统维护的内容**  1.纠正性的维护  纠正用户在使用系统软件过程中发现的错误。  2.适应性维护  当用户的硬件环境因升级或更换发生变化，承诺对系统进行适应环境变化的适应性维护（包括用户机构变化的系统迁移）。  3.改善性维护  与原开发商协商，对用户原有系统进行相应的修改，深化完善系统功能，使应用系统能更好地满足业务管理需要。同时对使用过程中发现的各类问题进行修改完善，使其应用更方便、更稳定。  4.预防性维护  制定年度预防性维护计划，提供每季度一次的预防性维护，对系统运行形成的临时数据进行清理，对系统运行日志进行检查分析，根据系统的报错信息，发现系统潜在的问题，尽早采取措施，排除故障隐患和安全漏洞。要求维护后提交完整的报告。  5. 数据的维护  对应用系统提供每季度一次的性能测试和调优服务，提供性能测试报告及系统性能优化建议，以便保证系统性能不断改进并运行在最佳状态。与原开发商协商，对系统的运行数据库数据进行优化及备份；进行程序代码优化，数据库代码优化，整合SQL，确保代码能在最短时间内运行。避免重复代码、无用代码等，跟踪异常处理等；对数据库进行优化，包括表结构优化，数据查询慢等进行优化。协助进行新增数据监督入库，定期数据库备份。  6.重要时刻保障  如有重要参观演示任务，应根据用户的要求派驻技术人员在现场职守。  7.咨询及培训服务  要求服务方提供电话或现场技术咨询和技术支持服务，同时，定期对用户的技术人员进行系统维护技术方面的培训，如一般故障排除方法，性能的监控与调整等。至少提供2 人系统管理员培训。  **2.1.2基础支撑系统运维服务**  本运维硬件主要包括网络设备、信息安全设备、监控设备及大屏幕。   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 序号 | 类别名称 | 投入使用时间 | 投入使用时长（月） | 数量 | | 一、网路设备 | | | | | | 1 | 交换机 | 2011/11/18 | 115 | 3 | | 2 | 核心交换机 | 2010/11/18 | 127 | 1 | | 3 | 路由器 | 2011/11/18 | 115 | 1 | | 4 | 接入交换机 | 2011/11/18 | 115 | 4 | | 5 | 网络OPE交换机 | 2019/4/28 | 26 | 1 | | 6 | 流控路由 | 2019/4/28 | 26 | 1 | | 7 | 24口POE交换机 | 2019/4/28 | 26 | 1 | | 8 | 交换机 | 2019/4/28 | 26 | 1 | | 9 | 路由器 | 2019/4/28 | 26 | 1 | | 10 | 无线AP | 2019/4/28 | 26 | 9 | | 二、信息安全设备 | | | | | | 1 | 防火墙 | 2020/11/10 | 43 | 1 | | 三、其他设备 | | | | | | 1 | 信息点 | 2010/4/16 | 134 | 100 | | 1 | 监控设备 | 2011/6/22 | 120 | 1 | | 2 | 视频监控设备 | 2019/4/28 | 26 | 1 | | 3 | LED大屏 | 2019/4/28 | 26 | 1 |   硬件运维需求表   |  |  |  | | --- | --- | --- | | 序号 | 服务内容 | 维护要求 | | 1 | 设备日常维护 | 1.工作内容：提供5\*8小时服务。非工作时间或节假日提供热线或电话支持服务，如有需要，须现场解决。  2.巡检周期：每月一次 | | 2 | 设备故障检测及排除 | 响应时间及排除故障时间：不影响业务正常开展的故障，在工作日内4个小时内解决，影响到业务正常开展的故障，在工作日内2个小时内解决。要求信息系统在线使用率达95％以上。达到100%的用户响应度。维护服务用户满意度不低于95%； | | 3 | 设备维保及备件提供 | 1.维保要求，时间响应要求  2.备件要求，24小时 | | 4 | 驻场要求 | 1.驻场  2.驻场人员数量 1名  3.驻场时间：8\*5 |   **设备维护内容如下：**  （一）在响应时间内完成上述范围的网络故障的分析和修复；属于后台核心网络问题的及时通知用户具体责任人员；  （二）在用户授权下，进行桌面设备的网络配置、调试；  （三）负责更换故障网线、调测不稳定端口、优化网络配置和部署；  （四）定期检查站内网络健康状况，及时发现和协助解决存在的问题，形成网络维护配置管理手册。  **2.2桌面运维服务**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 服务对象及人数 | 服务地点 | 所维护的设备数量（台） | 是否驻场 | 运维工作量（人月） | | 110服务对象及35人员 | 办公场所 | - | 是 | 12 |   **2.3网络安全服务**  **2.3.1网络安全服务**   |  |  | | --- | --- | | 安全服务内容 | 服务要求 | | 安全巡检服务 | 服务器和相存储设备巡检  网络和信息安全设备巡检 | | 安全漏洞扫描服务 | 系统漏洞扫描  数据库扫描  应用安全扫描 | | 安全加固服务 | 服务器安全加固服务  数据库系统安全加固  关键网络设备加固  安全设备加固 | | 安全通告服务 | 每季度通过邮件或传真方式提供安全通告 | | 应急响应服务 | 为系统发生的重大安全事件提供应急响应服务 | | 应急演练服务 | 通过测试与演练工作，提高应急响应人员的应对信息安全突发事件的能力，及时发现各部门应急过程中可能存在的不足和缺失，并依此对安全应急面临的现状进行持续改进。 | | 安全保密检查服务 | 提供安全保密检查服务所需的人力支持 | | 志愿时评测管理系统需要进行等级保护评测 | 差距测评  测评验收 | | 日志审计服务 | 含支持50个日志源的许可证书，支持获取各种主流安全设备、网络设备、主机、操作系统以及各种应用系统产生的海量日志，支持syslog，sftp，jdbc协议采集日志，支持日志归并和过滤降噪，通过内置和自定义解析规则支持直接解析和补全解析，支持类似google的自定义快速查询日志。 | | 安全管理平台服务 | 通过内置和自定义告警规则进行实时分析触发告警，支持告警合并，告警具备攻击图可视化能力，展示知识库、告警关联的日志等相关信息，支持以告警页面、邮件、SYSLOG、SNMP Trap、脚本执行、短信、告警铃等各种方式输出告警，通过内置和自定义报表具备多维丰富的全时空可视化安全风险呈现效果，系统支持三权分立、部门级数据权限、自动备份保障自身安全。支持界面自定义添加索引字段及索引去重，满足灵活性及易用性 | | 数据库审计服务 | 支持5个数据库审计，峰值事件处理能力3500条语句/秒，存储20亿条日志，采用旁路镜像网络流量采集数据库操作行为日志，无需在数据库上安装任何插件，对系统零影响；支持主流数据库类型：Oracle[8i、9i、10g、11g]， SQL-SERVER， MYSQL， Informix，SyBase， DB2；支持资产管理、系统查询、告警处理、报表展示、系统管理及监控；通过内置和自定义告警规则进行实时分析触发告警，支持以告警页面、邮件、SYSLOG、SNMP Trap、脚本执行、短信、告警铃等各种方式输出告警，通过内置和自定义报表具备多维丰富的可视化安全风险呈现效果，系统支持三权分立、数据权限、自动备份保障自身安全。 |   **2.3.2信息安全管理服务和安全培训**  1.服务方式  7×24小时热线支持、5×8小时现场支持、7×24小时远程支持等。  2.信息安全服务的内容  （1）安全巡检  通过及时发现存在的安全隐患，并根据运维现状提出合理的安全建议和措施。以降低我中心IT环境的安全风险，具体服务内容如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 信息资产 | 基线审计 | 对服务器、安全设备和网络系统进行专业检查和分析，对系统警告、异常情况、错误信息进行分析，发现可能存在的隐患，做到事前预防 | 人员要求：由高级工程师执行；  执行频率：要求每月进行一次，工作完成后5天内提交巡检报告。 | | 策略优化 | 根据分析结果对安全策略进行调整和优化，对服务器和网络系统提出安全加固与整改建议 | | 服务报告 | 提交巡检服务报告 |   （2）漏洞扫描  利用安全检测工具，对我中心的系统、主机、网络设备进行脆弱性和配置的合规性进行检测，及时发现问题，以降低因信息资产本身的脆弱性和不合规的配置带来的安全风险，具体服务内容如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 信息系统 | 资产识别 | 包括资产识别以及客户授权、实施工作计划等 | 人员要求：由高级工程师执行；  执行频率：要求每月进行一次，工作完成后5天内提交扫描报告。 | | 主机系统安全扫描 | 利用漏洞扫描系统对服务器的操作系统、网络设备、安全设备的各类安全问题测试，测试内容包括共享目录、账户信息、账户口令、系统漏洞等系统基本信息进行扫描。 | | 数据库漏洞扫描 | 利用漏洞扫描系统对服务器运行的数据库系统进行安全测试，测试内容包括数据库帐户安全、漏洞测试等。 | | 应用安全扫描 | 利用漏洞扫描系统针对服务器运行的基本应用服务（WEB 、DNS、FTP）进行安全测试，测试内容包括帐户安全、应用脚本安全测试。 | | 安全扫描报告 | 根据扫描结果，组织综合关联分析，并提交扫描报告 | | 安全加固方案 | 根据扫描报告提出安全加固方案及建议 |   （3）安全加固  通过对信息系统的漏洞跟踪及配置缺陷情况，提供各层次的专业加固服务，全面提升信息系统的安全保障能力。提高主机与系统运行的安全性、可靠性，具体服务内容如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 信息系统 | 确定加固范围 | 根据需要进行安全加固的系统的实际需要，划定加固范围。要综合考虑相关联的系统，不能在加固过程中对其他系统产生任何不良影响 | 人员要求：由高级工程师执行；  执行频率：要求每月进行一次。 | | 状况评估 | 对加固范围内的目标进行状况采集，包括取得系统的各种设计文档、使用手册、维护手册、系统日志，并与系统管理员进行交流，获得第一手的系统运行情况。 | | 加固建议实施 | 在实际的系统中实施加固之前，先要建立能够模拟真实系统的环境，在此环境中进行加固实施，通过后按照加固实施计划对实际的系统实施加固。 | | 加固记录 | 加固实施过程中，详细记录每一个步骤的工作内容和结果。 | | 跟进监督 | 加固实施过程中，详细记录每一个步骤的工作内容和结果，并持续跟进 |   （4）安全公告  通过不断跟踪安全技术的发展和新漏洞的出现，结合我中心信息系统的信息资产情况提供相应的安全信息通告。包括主流厂商的中文安全通告、其他应用系统和安全组织的安全通告、操作系统、数据库、常规应用系统补丁升级、网络安全漏洞、杀毒软件最新补丁包的更新信息、新病毒信息、新黑客技术、国际信息系统安全最新技术、安全技术的最新发展情况通告、最新公布漏洞及解决方法安全通告、最新的病毒动态及防治，具体服务内容如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 信息系统 | 安全资讯收集 | 通过各安全平台收集最新漏洞、病毒以及安全资讯信息，包括：主流厂商的中文安全通告、其他应用系统和安全组织的安全通告、操作系统、数据库、常规应用系统补丁升级、网络安全漏洞、杀毒软件最新补丁包的更新信息、新病毒信息、新黑客技术、国际信息系统安全最新技术、安全技术的最新发展情况通告、最新公布漏洞及解决方法安全通告、最新的病毒动态及防治、对于影响力大的计算机病毒24小时内提供具体的检测和修复办法、安全产品推荐。 | **人员要求：由**中级工程师执行；  **执行频率：**要求每季度提供一次服务，出具安全公告。 | | 信息关联分析 | 组织安全团队根据安全资讯信息进行关联分析 | | 安全公告 | 编写安全公告并发布 |   （5）协助安全保密检查  按照全市信息安全保密检查要求，配合我委开展内部信息安全保密自查和整改服务，确保我中心信息安全保密工作符合相关要求，确保顺利通过全市信息安全保密检查，具体服务内容如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 所有非涉密办公电脑、移动存储介质及工作邮箱 | 存储情况  检查 | 检查非涉密计算机终端，搜索是否存储国家秘密信息，包括图片格式的文件以及涉密文件的过程文件，存储介质使用记录，判定是否存在交叉使用情况 | 人员要求：中级工程师执行；  执行频率：按上级要求进行，全年不超过2次，工作完成后5天内提交安全保密检查报告。 | | 信息系统连接情况检查 | 查看网络拓扑，观察机房布线，重点关注核心网络设备是否与其它网络相连 | | 共用设备情况检查 | 打印机、复印机是否存在涉密计算机和非涉密计算机共用情况 | | 安全服务  报告 | 综合安全保密检查各项数据进行总结报告 |   （6）应急响应服务  协助我中心建立完整的应急响应机制，为我中心提供重要信息安全保障时期和重大信息安全事件时的应急响应和现场技术支持服务，具体服务内容与要求如下：   |  |  |  |  | | --- | --- | --- | --- | | **服务对象** | **服务分解** | **服务说明** | **服务要求** | | 信息系统 | 应急准备 | 包括建立应急响应组织、制定应急响应制度、划分应急事件级别以及预案管理等等 | 人员要求：由中级工程师和高级工程师执行；  执行频率：按需提供服务，全年不超过4次，工作完成后1天内提交应急处置报告。 | | 事件研判 | 事件等级判定、应急方案制定 | | 应急处置 | 发生应急事件进行排查诊断、处理恢复，事件升级以及事件关闭工作。 | | 总结改进 | 应急工作总结及改进 |   （7）安全培训服务   | **序号** | **服务名称** | **服务内容** | **备注** | | --- | --- | --- | --- | | 1 | 安全培训服务 | 以信息系统实际业务运作为立足点，注重理论和实际结合，通过理论讲授、实验操作、问题讨论等方面，普及安全教育，提高安全意识，提高安全防范能力。  安全培训服务应提供包括用户相关人员参加的分批分级的网络安全的相关法律法规培训、各种网络攻击技术原理及防御培训、网络安全策略及安全管理培训、常用网络安全产品原理及应用培训等服务。 | 提供《安全培训服务报告》。 |   **2.3.3等保差距测评**  2022年志愿者行动指导中心信息系统等保测评服务部分主要针对以下系统进行等保评测服务：   | **序号** | **系统名称** | **等保定级** | | --- | --- | --- | | 1 | 应用系统 | 三级 |   （一）计划在2022-2023年等保测评具体实施内容如下：  1.对以上信息系统安全等级保护状况进行测试评估，主要包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。  2.对安全控制测评的描述，使用测评单元方式组织。测评单元分为安全技术测评和安全管理测评两大类。安全技术测评包括：物理安全、网络安全、主机系统安全、应用安全和数据安全等五个层面上的安全控制测评；安全管理测评包括：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全控制测评。  **2.3.4数据安全管理要求**  为降低开展信息安全服务工作过程中对数据安全的风险，针对本次项目的数据安全管理工作提出如下要求：  （1）提供数据安全恢复、数据保密及数据灾难抢救的服务，确保数据使用的高安全性、高保密性。  （2）系统需提供由国家信息中心信息安全研究与服务中心（或者国家级数据恢复涉密机构）提供的1年或以上的数据恢复服务，投标人必须承诺中标后签订合同前提供国家信息中心信息安全研究与服务中心（或者国家级数据恢复涉密机构）的数据安全恢复承诺函原件。  （3）为本项目提供数据恢复的机构必须具有国家保密局颁发的关于“数据恢复”的相关资质证书，投标时提供证书复印件。  **三、质量控制**  每个阶段必须有明确的《阶段计划》，包括：阶段目标、阶段时间进度、工作任务和人员的任务等内容。  每个阶段必须有相应的《工作日志》、《考勤登记》、《工作完成情况登记》和必要的《工作备忘》等文档材料。  每个阶段的结束都必须进行评审和确认，对本阶段的工作进度、质量和完成情况进行评审，形成《阶段评审确认书》，为下一阶段工作打下良好的基础。  每一阶段的运作过程必须是有组织、责任明确、顺畅执行和留有书面记录的。  **四、进度控制**  1.记录审核  服务过程中产生的各种记录、报告和分析过程表格必须形成文档，文档由服务的负责人签名与审核，项目监管人员将定期检查相应的记录确认各项记录的完整性。  2.流程监督  质量管理团队将定期对服务项目进行审核，审核将包括流程是否得到正确实施，结果是否符合规定的标准。审核将要求服务提供者能够提供证据证明流程已经得到正确的执行，服务质量有相应的保证。  3.阶段评审  服务提供过程中，质量管理团队将定期对服务的质量进行阶段评审，由用户、质量管理团队，服务项目团队共同对服务质量进行评价，对出现的偏差提出整改意见，并对下一阶段的工作做出规划。  4.异常处理  当质量管理团队发现异常状况出现后（未按流程进行工作、超过期限），首先与服务项目负责人进行沟通，要求对项目进行整改，做出相应的补救措施，并进行记录；如果异常情况可能影响服务的质量，则应当立刻向项目最高领导人进行汇报，或要求召开项目临时会议，由用户与服务方共同对项目计划进行调整。  **五、合同管理**  双方签订的合同文件按要求进行归档。  **六、项目信息管理**  运维单位不得泄露业主信息资料,未经业主同意不得将有关信息资料用于第三方。  **七、项目文件的管理**  1.维护人员对出现故障的计算机维护后需登记到相应的记录清单上；  2.日常检测必须将检查结果登记到相应的维护记录清单上，并与每周五下班前将记录清单交由维护负责人检查并签字确认。  **八、项目安全的管理**  运维单位定期检查网络是否被入侵,并保障整个单位的网络信息安全。  **九、知识产权的管理**  所有知识产权归业主所有。 | | | | | |
| 对运维单位的要求 | | | | | |
| 对运维机构的管理架构要求  本项目的配置人员主要包括两部分：业务操作人员和技术支持人员。技术支持人员需要了解系统的详细内容，并提供系统的管理维护及对业务操作人员的技术支持 | | | | | |
| 对运维单位的人员要求 | | | | | |
| 人员类别 | | 数量 | 人员要求 | | |
| 项目经理 | | 1 | 1.具有：计算机软件高级系统分析师、软件工程造价师、信息系统项目管理师、一级建造师（通信与广电）、安全生产考核合格证（建安B证及以上）等技术或管理相关资质证书；  2.其他要求：  （1）具有较全面的ITIL运维管理知识。  （2）熟悉业务应用软件开发和维护工作。  （3）熟悉相关规范标准。  （4）熟悉管理工作，具多年的项目管理工作经验 | | |
| 驻场运维工程师 | | 1 | 1.具有IT服务工程师、中级工程师及以上等资质证书；  2.其它要求：  （1）未经业主批准，不得随意更换驻场运维工程师；  （2）供应商应保证能根据项目建设的实际需要，在相应阶段安排足够的运维工程师到场开展工作。  （3）驻场工程师应该具有在计算机及其设备硬件技术、操作系统软件、常用应用软件、网络技术、安全技术、系统运行与维护工作管理方面具有非常专业的经验和知识，有相关工作经验。  （4）服务商派到甲方的驻场工程师，要求该人员的任用符合劳动合同法及地方劳动部门的相关规定，按规定购买社会保险及公积金等劳动保障项目，人员进场时应该提供相关的社保和合同等证明文件。（5）服务商派到甲方的驻场工程师，接受采购单位的管理，必须遵守甲方相关的规章制度及相关的保密规定，采购人对驻场工程师的表现不满意有权要求供应商更换。  （6）驻场工程师须自觉主动进行日常常规的巡检和维护保养工作，完成采购单位交与的计算机及网络的相关工作。  （7）服务商提供1名专职技术工程师常驻现场，协助用户开展日常运维工作。 | | |
| 二线支持工程师 | | 2 | 1. 具有高级工程师及以上职称、注册信息安全工程师证书、信息安全保障人员认证证书；  2.其他要求：安排2人的二线技术支持服务组，参与本项目日常巡检、突发事件、应急事件服务工作。本项目的技术人员和项目负责人必须固定，如有变更，必须经用户同意并签字确认。供应商必须提供人员管理及配备方案，并确保其人员的稳定性。 | | |
| 其他人员 | | / | / | | |
| 对运维单位的设备投入要求： | | | | | |
| 1.为确保安全服务工作的稳定推进，要求供应商在服务期间提供专业服务工具（供应商在服务期内免费提供给采购人使用，无产权要求）  2.专业服务工具清单（供应商在服务期内免费提供给采购人使用，无产权要求）   |  |  |  | | --- | --- | --- | | 序号 | 产品名称 | 数量（套） | | 1 | 智能IT服务管理系统 | 1 |   3. 智能IT服务管理系统技术要求：   |  |  |  | | --- | --- | --- | | **序号** | **功能模块** | **技术要求** | | 1 | 事务管理 | 全生命周期的事务管理，自动化的工作流提高IT运营效率 | | 2 | 知识库 | 集合多个层面的海量知识管理，互惠互利的知识分享机制，可以有效地利用这些知识库，搜索想要的信息。 | | 3 | 问题管理 | 对问题进行分类、分析和解决。 | | 4 | 配置管理数据库 | 全面追踪和管理所有IT配置项，映射配置项之间的关系及依赖性。 | | 5 | 变更和发布管理 | 通过自动化的工作流简化规划、审批和实现。消除未授权和失败的更改。 | | 6 | IT项目管理 | 创建项目，管理资源并跟踪项目进度。 | | 7 | 服务目录 | 依据自定义的SLAs协议，创建和发布服务目录，全面展现服务内容。 | | 8 | 仪表板和报表 | 提供全面的报表，满足从不同视角查看/分析帮助台数据的要求。从而为量化管理、决策制定提供参考数据。 | | 9 | 用户自服务 | 可以通过自助服务门户，提交事务单、查看事务单处理状态、查找常见问题的解决方法，从而减轻帮助台负荷。 | | 10 | 智能创建和分配失误 | 与ITOM或其他系统对接，机器深度学习历史处理规则，分析系统警告和错误信息，根据工作负荷、可用性以及SLA服务级别要求，智能创建和自动分配事务单。 | | 11 | 通知提醒 | 在创建或分配事务时，通知IT技术人员，并让用户通过微信、邮件、手机短信获知每一步的状态。 | | 12 | 用户满意度调查 | 通过满意度调查，获得反馈，了解满意度。可配置发送调查的时间，比如在事务单关闭时发送。 | | 13 | 业务规则 | 配置业务规则来组织需求，对符合业务规则的请求进行智能分类和自动标识状态，实现无人值守的智能化管理。 | | 14 | 微信小程序 | 利用微信小程序报告故障、提出需求，用户和IT人员可以随时查看和处理事务，提高满意度。 | | | | | | |
| 服务响应要求 | | | | | |
| 1.影响到业务正常开展的故障，30分钟内到达现场，60分钟内报告采购方主管负责人，2小时内安排资源解决。如不能解决，需要二线技术人员提供现场技术支持服务，最迟在8小时内解决问题。在故障解决过程中，保持每4小时内1次与客户进行情况汇报。  2.不影响业务正常开展的故障，120分钟内到达现场，4小时内报告采购方主管负责人，1个工作日内解决。  3.党政机关系统办公自动化设备运维项目适用如下条款：  ★供应商为广州市涉密设备维修维护定点单位的，在报价文件中提供《广东省涉密计算机、通信和办公自动化设备定点维修维护证书》【以广州市保密局《转发省保密局关于富士施乐办公自动化设备落实定点维修维护有关问题的通知》（穗保密局〔2013〕9号）公布的名单为准】；如非广州市涉密设备维修维护定点单位的，须委托广州市涉密设备维修维护定点单位对所投产品进行免费印量、全包服务等维修维护工作【在需求文件中提供受委托维修维护单位的《广东省涉密计算机、通信和办公自动化设备定点维修维护证书》和委托合同（为保证涉密设备维修维护定点单位的维保质量，供应商提供的委托合同必须涵盖委托维修维护单位的响应时间、服务承诺、维修质量保证等内容）】 | | | | | |
| 项目考核要求 | | | | | |
| 1. 总体要求   1.组建专业服务团队，定期对用户信息化设备开展巡检，对设备故障提供现场的及时响应。提供电话技术及上门支持服务，解决设备故障。  2.提高设备维护维修效率，建立完善的设备维护维修流程体系，加强服务维修时间及服务水平承诺管理，提供相应备件支持，提高事件解决以及维修速度。  3.加强用户对信息化设备的使用与运维管理。统计信息化设备维护、损坏情况，为信息化规划提供决策依据。提高信息化设备的使用效率，减少设备停机时间，减少对用户的办公影响，节约财政资金，减少国有资产流失。   1. 绩效评估   1.应能在10分钟内准确诊断并告知用户故障原因，诊断差错率要控制在5%以内。并向最终用户解释故障发生原因，可能导致的后果，以及拟采取的措施。  2.故障修复过程中可能影响用户工作或对系统应用数据有影响的，要先咨询用户意见再处理。  3.如果配件需要送修或更换，维修期间提供同档次的备用设备，并需要配合用户登记故障配件的型号和产品序列号，并由用户签字后再送维修。  4.如果机器送修，需要保护好磁盘等存贮设备。要先将用户数据备份好，再送维修。  5.建立巡检制度：所有设备进行季度的巡检检查，记录设备状况，列出注意事项，并反馈给用户。  6.设备维修结束后，维修人员需向用户出示服务维修单。服务维修单上需注明维修日期、维修人员、维修地点、故障、故障原因分析、修复结果等。  7.更换配件及设备维修的费用由我处承担。  8.在每个结算周期中，单位监管部门接到有效投诉超过5次，用户方有权中止与维护方的合约。  9.维护方须向用户提供项目负责人及维护人员的详细联系方式。  10.响应类型要求：热线电话、手机支持，上门现场解决  11.服务类型要求：送修、现场、特殊服务要求（如购件、升级等）  12.现场维护确认表：工程师现场维护填写现场维护表，故障排除后由用户签名确认。 | | | | | |
| 测试与验收 | | | | | |
| 供应商应根据所提交的验收方案和实施办法，自行组织设备和人员，并在使用单位监查下现场进行测试和验收。 | | | | | |
| 培训要求 | | | | | |
| （一）目的  使之能够顺利地实施项目咨询、体系建设和更好地配合和理解运维体系和流程；使采购人掌握对信息化系统的使用及维护。  （二）培训要求  对系统管理员进行充分的技术培训，保证管理人员掌握必要的技术、管理工具，通晓管理规范。  （三）培训师资  供应商派出具有相应专业资格和实际工作经验的教师和相应的辅导人才，主要的培训教员均获得相应的资格认证并且具有 3 年的实际教学经验。培训使用的语言和教材均为中文。  （四）个人应用培训  供应商在运维服务过程中将根据采购人终端用户服务申请情况予以分类，进行个人应用培训，培训周期：至少每 12 个月一次。  （五）费用  供应商应将所有培训费用（含培训教材费）及各项支出费用分别报价并计入总价。 | | | | | |
| 付款方式 | | | | | |
| 1．本合同签订后15个工作日内，采购人办理财政集中支付手续，向供应商支付合同总额的80%；  2．服务期每满12个月后，由采购人组织服务验收，在10个工作日内根据绩效评估等级确定的付款比例申请财政支付合同金额的15%；  3．当服务期满并通过项目终验后，在10个工作日内申请财政支付合同金额的余款5%。  4．达到支付条件后，运供应商须在采购人办理付款手续之前7个工作日内，提供等额的正式发票给采购人，以便采购人办理付款手续。 | | | | | |