深圳市档案馆2021年信息化日常维护项目招标文件

2021年1月

目录

一、 项目概况 1

二、 项目预算 1

三、 投标人资质要求 1

四、 服务内容 2

（一）桌面终端与外设维护服务 2

（二）网络和机房设备维护 4

（三）日常IT配件采购 5

（四）安全专项服务 5

（五）信息安全检查相关服务 7

（六） 设备原厂维保服务 12

（七） 信息安全软件授权服务 12

五、 技术要求 13

（一）人员要求 13

（二）服务实施能力要求 14

（三）服务方案技术要求 14

六、 商务需求 15

（一） 服务期 15

（二） 报价要求 16

（三） 付款方式 16

（四） 实质性响应条款偏离表 17

（五） 风险责任 17

七、 开标、评标和定标 18

（一）开标 18

（二）评标 18

（三）定标 19

八、 投标文件 22

九、 其他要求 24

# 项目概况

深圳市档案馆包括计算机、网络、服务器、存储设备、安全设备及软件系统的等全套IT环境及其信息安全的维护。

# **项目预算**

项目预算人民币玖拾万元整（￥900,000.00元整）。

# **投标人资质要求**

（一）投标人必须为在中华人民共和国境内注册并合法运作的独立法人（须提供营业执照复印件或扫描件加盖投标人公章）；

（二）具有国家信息安全测评中心颁发的《信息安全服务资质安全工程类》或国家信息安全认证中心颁发的《信息安全服务资质认证》证书（提供证书复印件或扫描件加盖投标人公章）；

（三）参与政府采购项目投标的供应商近三年内无行贿犯罪记录（投标人提供书面声明）；

（四）本项目不接受联合体投标，不允许分包、转包。

# **服务内容**

## （一）桌面终端与外设维护服务

深圳市档案馆办公信息化设备，包括台式电脑、笔记本电脑、打印机、显示器等终端和外设的维护，驻点服务。包括设备的维修（不含配件），操作系统、杀毒软件、办公软件、业务软件的安装维护等。涉及的终端设备约250台，打印机约100台。工作内容包括但不限于以下内容：

1.负责所有需维护的电脑及相关设备的硬件安装调试、检测、维护，对设备使用过程中出现或存在的故障进行及时诊断、维修；对在保修期内的硬件故障通知原厂家或第三方质保厂家维修，并对厂家维修情况进行跟踪、落实和汇总。具体硬件维护服务内容包括：

（1）台式电脑：主板、CPU、硬盘、内存、显卡、声卡、网卡、隔离卡，光驱、软驱、MO驱动器、内置刻录光驱、MODEM卡、电源、所有外接端口；

（2）笔记本电脑：显示液晶屏、主板、CPU、硬盘、内存、显卡、声卡、网卡、光驱、软驱、MO驱动器、MODEM卡、电源、所有外接端口；

（3）服务器：主板、CPU、硬盘、阵列卡、内存、显卡、声卡、网卡、光驱、软驱、MO驱动器、内置刻录光驱、MODEM卡、电源、所有外接端口；

（4）打印机：主板、外接端口、内存等非耗材零配件；

（5）显示器；

（6）设备内外清洁；

（7）存储设备驱动器清洁，硬盘、磁带更换，配置；

（8）其他外设设备。

2.负责所维护的电脑及相关设备的软件安装、调试、升级工作，对设备在使用过程出现或存在的故障进行及时诊断及排除，在技术可行的条件下对用户误删除的数据进行恢复。具体软件维护内容包括：

（1）办公、系统类软件维护：操作系统、办公软件、OA系统、业务相关软件等；

（2）工具类软件维护：输入法、压缩软件、图像处理软件等实用性软件；

（3）安全类软件：防病毒软件、准入控制软件等；

（4）病毒检测及病毒的紧急处理；

（5）主机性能诊断；

（6）系统软件检测及重新安装；

（7）其他应用软件的安装、设置；

（8）外围设备连接、安装驱动及检查；

（9）设备正常操作方法的简单培训。

3.负责所维护的电脑及相关设备的网络连接安装、调试及检测工作，对设备在使用过程中出现或存在的网络故障进行及时的诊断及排除，包括对设备所连接的相关信息点的线路诊断及故障排除，以及楼层网络接入的维护。涉及网络主要为政务公共网、政务办公网、馆内局域网。

## **（二）网络和机房设备维护**

深圳市档案馆网络、网络设备、安全设备、服务器、存储设备等的日常维护。涉及网络主要为政务公共网、政务办公网、馆内局域网；涉及服务器和存储设备约45台，及网络设备、安全设备、备份设备若干；设备品牌有华为、联想、浪潮、绿盟、天融信、锐捷等。服务包括设备检查、维护、维修，操作系统、数据库软件、安全软件、会议系统等的安装、更新、维护等，及机房（含托管机房）和相关设备间的日常巡检和管理，驻点服务。确保市档案馆的网络通畅，设备正常运行。主要内容包括网络维护、设备基础维护、软件基础维护、巡检和应急响应，具体如下：

1.确保深圳市档案馆内各网络安全畅通，确保网络、安全设备、服务器、存储设备及虚拟化系统、网络管理软件系统和其他软件系统等正常运行，提供7天24小时响应服务；网络系统主要涉及深圳市档案中心ABCD四座楼宇及其与市大数据资源管理中心的连接。

2.对设备实行定期的预防性维护(每月一次)，每季度进行一次设备、网络巡检，向采购方提供巡检报告和改进建议，并按采购方要求实施改进工作。

3.每季度进行数据库的巡检维护，数据恢复和性能调优工作。提交《季度服务器及数据库巡检及优化报告》。根据数据库和应用系统情况、存储容量变化、应用的变化情况对数据库提出调整建议及做出调整。

4.日常巡检。每工作日安排对机房和设备间进行2次巡检，查看设备和机房环境状况是否正常，发现异常情况时马

上记录，并及时报告处理，建立巡检台帐备查。长假期间须按采购方要求进行巡检。

5.应急响应。发生断电、漏水、温度超标及其他紧急状况时（包括非工作日、夜间），必须派人立即至现场查看情况、向采购方汇报并按要求进行处理；及时维修、处理故障设备；出现灾难性故障时现场协助系统和数据的恢复工作，保障数据库系统的正常运行。

6.配合采购方实施数据备份和数据清理。

7.配合采购方进行数据库调优。

8.免费提供必要的数据库补丁升级安装服务。

9.技术支持：负责解答采购方提出的问题，无限次电话及邮件支持。

## **（三）日常IT配件采购**

为确保设备故障时能够及时更换配件，该项目中安排9万元用于日常设备维护维修的相关配件的采购，中标方从正规途径采购原装正品配件并以成本价提供，到用户现场调试安装；中标人必须保证配件与设备匹配及安全可靠。投标人报价时，需注意，本项目服务配件采购费用的报价需保证在人民币9万元或以上，按实际发生金额结算。

## **（四）安全专项服务**

通过安全专项服务，实现整体安全管理制度建设、安全体系建设、安全体系咨询等服务。

1.安全顾问服务：主动对网络安全改善提出合理性的建议，制订基于网络环境、应用需求、业务流程、组织结构和战略目标的安全策略与实施计划，并详细说明实现安全策略的方式方法。提供包括安全管理体系设计、安全技术选择和推荐、安全管理制度的制定、灾难恢复计划咨询等服务。

2.信息安全资料服务：按采购方要求提供信息安全的国家政策、法规、标准的文本和解读，定期提供最新的安全动态、技术资料等。

3.终端安全保密检查服务：每季度对采购方的所有计算机等终端设备进行安全保密检查，并根据检查情况进行修复整改，并建立安全检查、整改台帐和采集记录终端设备信息。

4.安全培训服务：邀请政府安全机构、部门专家，通过理论讲授、问题讨论等方方式，对采购方开展全员培训，建立培训台帐，普及安全教育，提高安全意识，提高安全防范能力；以实际业务运作为立足点，注重理论和实操结合，组织信息化工作人员进行专业的信息安全培训，颁发培训证书。

5.安全管理策略服务：建立安全管理策略，主要针对人员管理，机房管理，终端机管理。根据用户需求,协商制定,修改完善。

6.安全制度修订咨询服务：按照信息安全等级保护的要求，结合采购方的实际情况，提供修订相关的信息安全管理制度的咨询服务。

7.信息安全应急处置服务：在采购方遭遇信息安全事件时，应快速反应，提供技术支持并派出安全工程师协助采购方处置。

## **（五）信息安全检查相关服务**

1.为确保采购方信息系统的稳定、安全运行，结合深圳市委、市政府和市信息安全主管部门要求，依据国家、深圳市信息安全相关政策法规和指引文件，针对采购方信息系统进行信息安全风险评估、信息安全制度落实情况、安全防范措施落实情况、应急响应机制建设情况、信息技术产品和服务国产化情况、安全教育培训情况、责任追究情况、安全隐患排查及整改情况等与信息安全检查相关的安全服务和绩效评估信息安全顾问服务，对安全服务过程中发现的脆弱点和问题提出科学、可行的修复加固计划和建议，建立符合国家标准和深圳市电子政务要求的信息安全管理体系，并在一年的服务期内，使系统的安全状况得以长期保持。服务范围和项目实施要求参照2021年深圳市委、市政府和市信息安全主管部门印发的信息安全检查相关文件为准。

2.安全服务内容

| 序号 | 大类 | 描述 | 子类 | 工作内容 | | 全年次数 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 信息安全风险评估 | 以信息资产为主线，分析信息系统可能面临的威胁，当前存在的弱点，以及弱点被威胁所利用的可能性及影响，以此为基础对当前信息系统的安全风险进行分析和定义。服务要求参照我市信息安全联合检查相关文件。 | 资产分析 | 分析所有信息资产（包括硬件、软件、文档和数据、人力、业务应用、物理环境、组织管理等）的保密性、可用性、完整性安全属性，确认关键资产 | | 1 |
| 威胁分析 | 对资产（包括硬件、业务应用、物理环境、组织管理等）面临哪些潜在威胁，导致威胁的问题所在，威胁发生的可能性有多大等问题进行分析 | | 1 |
| 弱点分析 | 从管理、技术两方面，全面分析系统存在的各种脆弱性，分析弱点被利用的可能性 | | 1 |
| 现有措施分析 | 分析已有的安全措施对安全风险的控制作用 | | 1 |
| 风险分析 | 计算并得出当前系统仍存在的风险，并给出相应控制和管理风险的建议 | | 1 |
| 评估报告 | 编写真实、全面、准确并符合深圳市信息安全风险评估指南要求的风险评估报告 | | 1 |
| 评估总结 | 编写真实、全面、准确并符合深圳市信息安全风险评估指南要求的评估总结 | | 1 |
| 2 | 信息系统加固修复 | 对在上年度发现的信息安全问题进行加固修复，包含但不限于各种信息安全检查、抽查整改、风评结论整改等。 | 信息安全整改 | 完善并落实上年度工作、信息安全检查、抽查中发现信息安全问题的整改工作 | | 1 |
| 信息安全风险评估不可接受风险整改 | 完善并落实上年度信息安全风险评估的不可接受风险整改工作 | | 1 |
| 管理加固 | 对现有信息安全管理体系中存在的问题进行优化和完善，并协助采购方完成相关文档的编写和宣传 | | 1 |
| 服务器加固 | 对全网的服务器进行修复加固和漏洞扫描。Windows服务器直接修复加固，非Windows服务器协助采购方或维护厂商完成修复加固 | | 1 |
| 网络加固 | 对全网的网络设备和安全设备进行修复加固和漏洞扫描 | | 1 |
| 应用系统和数据库系统加固 | 为所有B/S和C/S架构的应用系统提供修复加固技术支持和优化服务 | | 1 |
| 安全策略加固 | 确认主机操作系统、应用系统的安全策略未被更改或还原 | | 1 |
| 安全设备加固 | 对安全设备中的配置、策略进行加固修复 | | 1 |
| 3 | 信息安全制度自查与优化 | 建立与完善信息安全管理体系 | 信息安全制度自查 | 找出现有安全制度不足及与国家、省、市要求的差距。 | | 1 |
| 信息安全管理体系建设服务 | 建立与完善采购方的信息安全管理机构、信息安全管理制度，建立符合采购方信息系统现状的信息安全管理体系 | |
| 4 | 安全防范措施自查与优化 | 检查现有信息系统中安全防范措施的落实情况，对不符合检查要求的现状和措施进行优化和整改 | 外包软件安全检测 | 对采购方投入使用前的外包开发软件进行安全检测 | | 2 |
| 安全域划分与建设防护 | 对采购方网络信息系统进行科学、合理地安全域设计和划分 | |
| 对采购方网络各安全域进行科学、合理地定性定级 | |
| 编制各安全域的安全防护设计方案，并协助采购方实施 | |
| 向互联网发布的网站的安全测评 | 对采购方向互联网发布的所有网站进行安全测评 | |
| 保密检查 | 协助采购方保密部门，对涉密计算机和涉密存储介质进行检查。检查内容包括：非法外联、物理隔离、移动存储介质的混用、密件处理、监控软件状态等 | |
| 计算机资产统计 | 收集统计采购方在使用的计算机资下列信息，包含： 计算机主机名、计算机IP地址、计算机MAC地址、计算机使用人或责任人、计算机所属部门、计算机的物理位置；服务器的IP地址、MAC地址、安装应用、物理位置等。 | |
| 网站备案 | 完成采购方所有网站在公安网监部门的备案，并取得国际联网备案登记证书和备案编号等证明文件 | |
| 安全防范技术措施有效性检查 | 检查采购方信息系统现有安全防范技术措施的有效性 | |
| 5 | 应急预案建设与演练 | 建立符合信息系统现状的科学的应急预案，并制定演练计划进行预案演练和验证 | 应急预案制定 | 应急预案建设  对采购方所有重要信息系统和对公众服务的信息系统制定科学、有效的应急预案 | | 1 |
| 应急技术支援队伍的建设  针应急预案的特点，建立合理、高效的应急技术支援队伍 | |
| 应急预案演练 | 演练计划制定  对采购方所有重要信息系统和对公众服务的信息系统制定科学、合理的应急演练计划 | |
| 演练预案培训  就应急预案内容对信息化相关岗位人员进行培训 | |
| 应急演练实施  对应急预案进行演练，验证其可行性，并对发现的问题进行修正 | |
| 应急预案修订 | 结合应急预案演练情况对预案进行修订和完善 | |
| 6 | 信息安全预警服务 | 为采购方信息系统提供例行全面的专业信息安全服务 | 安全咨询 | 对系统改造、扩建，新系统的上线等提供技术论证和安全咨询 | 技术方案咨询：就新应用系统上线或网络结构改造、扩容等提供技术方案设计 | 不限次 |
| 技术论证咨询：对新的安全体系的技术特点、功能进行论证 |
| 技术交流咨询：就信息安全领域新的技术、体系与客户分享 |
| 安全通报 | 定期通报安全行业动态、系统漏洞和病毒预警信息 | 行业动态通报：对信息安全领域的动态进行通报 | ≥24 |
| 漏洞安全通报：对新出现的安全漏洞进行通报 |
| 病毒安全通报：对新出现的较严重病毒进行通报 |
| 7 | 微信公众号、微信小程序、手机APP安全检测 | 运行环境安全检测  软件自身安全检测  用户操作安全检测  数据安全检测  通信安全检测  业务安全检测 | | 通过全面深入检测，发现存在的安全问题，从而提升公众号安全现状水准及满足安全监管部门合规要求。 | | 4 |
| 8 | 其他信息安全相关服务 | 未在上述逐一列举的信息安全的其它服务 | | 严格、准时、优质的完成各项服务 | | 1 |

3.安全服务要求:

（1）信息安全风险评估要求

①风险评估的范围要全面包括采购方的所有信息系统资产；

②对政务办公网、政务公共网、局域网的服务器、网络设备、安全设备进行详细的安全风险分析；

③风险评估全过程产生的所有过程文档、原始数据、扫描报告、正式报告等必须进行电子和纸制双重归档，在项目结束后一并移交给采购方；

④担任采购方计算机网络和主机系统的安全顾问，在网络和主机系统进行升级、扩建时，提供安全风险评估，并提供安全修补建议。

（2）安全检测工具要求

投标人在项目中用于安全检测使用的安全产品必须为厂商正版授权、符合国家安全标准及采购方提出的有关质量标准的设备和产品，提供检测工具厂商的使用许可证明资料或与检测工具厂商签订的合同等证明资料，原件备查。

1. 微信公众号检测工具要求

投标时需提供移动安全漏洞扫描工具厂商出具授权书。

（4）信息安全服务要求

①安全防范技术措施落实情况的核查务必真实准确，确保在规定的时间内完成核查并汇总成册后上报；

②信息系统应急预案必须以信息系统真实业务流程为基础，要求真实、科学；

③信息系统应急预案演练过程文档、会议纪要、修订文档等必须进行电子和纸制双重归档，在项目结束后一并移交给采购方；

④服务范围和项目实施要求以市委办、市府办及信息化和信息安全相关部门等下发的关于深圳市党政机关信息安全联合检查工作的相关文件为标准。

## 设备原厂维保服务

购买重要设备的原厂维保服务1年。本次购买原厂维保服务的设备为：5台深信服超融合一体机aSever-2205，1套深信服桌面云系统平台。

## 信息安全软件授权服务

1.购买覆盖采购方政务公共网终端的企业版360（奇安信）安全软件授权服务3年；

2.购买覆盖采购方政务办公网终端的联软准入控制软件授权服务1年；

3.购买覆盖采购方局域网终端的企业版专用杀毒软件授权服务3年，要求软件支持无互联网升级。

以上软件授权需能覆盖采购方设备。

# **技术要求**

## **（一）人员要求**

1.至少2名现场驻点人员进行现场日常维护，为期一年，负责维护项目日常工作，驻点上班时间与采购方一致；投标人不得安排驻点人员承担与本项目无关的工作，否则视为违约。现场驻点人员要求至少1名具有项目经理或CISSP技术认证资格的工程师。并配备2名替补工程师，在原驻点工作人员不能到岗时替补，及驻点工作人员无法及时完成工作时临时增加驻点工作人员。

2.提供1名安全工程师专职负责招标单位的信息安全检查服务，为期一年，专职安全工程师需具有丰富的党政机关信息安全服务项目工作经验，具有CISP技术认证资格证书。

3.不得随意更换驻点人员，如因人员辞职等原因确实需要更换的，需提前一个月书面通知采购方，取得采购方签字同意后方可更换，更换工作人员必须做好交接工作。

4.驻点和信息安全服务人员必须随合同提供无犯罪证明并签署保密协议或保密承诺书；如有人员不能提供或拒绝签署保密协议（承诺书），应更换不低于其专业技术资质的服务人员。

5.投标人必须做好项目服务人员，特别是驻点服务人员和安全服务人员的日常新冠病毒防疫工作，人员离开深圳的，返回后应进行病毒核酸检测，并将检测报告提交采购方，检测合格后方能返岗。

## **（二）服务实施能力要求**

1.系统综合诊断定位故障能力。中标人应具有在数据库、主机、存储、安全、网络等关联产品系统领域深厚的技术积累能力，以保障服务故障的快速诊断定位与解决。

2.现场服务支持能力

（1）中标人应具备在全市范围内提供现场服务支持的能力；

（2）中标人应具备深圳市内现场服务网络，能够就近为采购方提供及时、高效的现场服务；

（3）中标人应具备在全市范围内提供损坏件更换支持的能力，对于不能在规定时限内解决的系统故障，必要时具有提供备机服务的能力。

3.服务管理能力

（1）专业服务管理机构:中标人应具备专业的服务管理组织机构，并建立有完善的技术服务管理体系；

（2）服务流程管理能力:中标人应具有专业的服务响应中心，能够7×24小时响应采购方的服务请求，并具有流程化的管理处理能力；

（3）服务质量控制能力:中标人应配备有专职项目经理、调配专业后备技术支持团队支撑项目，并有定期回访机制，确保服务质量。中标人需与采购方签订保密协议。

## **（三）服务方案技术要求**

1.响应支持服务

（1）电话支持服务：中标人应具备7×24小时的电话支持服务能力。对于实时性要求不高的服务，能够在每周一至周五，每天9：00-18：00随时响应采购方的服务请求，对于较为急迫的业务，做到每周7天，每天24小时响应采购方的服务请求，并立即提供电话支持服务。

（2）远程分析服务：在征得采购方允许的前提下，中标人的工程师能够通过远程拨入进行故障分析，对系统进行诊断与故障排除。

（3）现场支持服务：

①中标人应具备7×24小时的现场支持服务能力。对于实时性要求不高的服务，能够在每周一至周五，每天9：00-18：30随时响应采购方的服务请求，对于较为急迫的业务，做到每周7天，每天24小时响应采购方的服务请求，并立即提供现场支持服务。

②当通过远程支持不能解决问题或诊断有硬件故障，中标人应派出工程师立即赶赴故障现场进行紧急现场支持。

（4）故障级别与服务响应速度定义

当采购方的设备发生问题时，采购方可以自己确定问题的优先级，从而得到不同的响应速度。

# **商务需求**

## 服务期

本项目硬件及网络维护服务期为2021年全年，但因为涉及设备和系统较为复杂，驻点人员在服务期前后两周进行交接，特殊情况适当延迟交接时间，并无条件做好交接工作。

本项目是长期服务项目，合同期限可以延长，但最长不超过3年，具体期限由采购方根据中标供应商履约情况确定。

## **报价要求**

1.本项目服务费采用包干制，应包括服务成本、法定税费和企业的利润。由投标供应商根据采购文件所提供的资料自行测算投标报价；一经中标，报价总价作为中标供应商与采购方签定的合同金额，合同期限内不做调整。

2.投标供应商应当根据本企业的成本自行决定报价，但不得以低于其企业成本的报价投标。

3.投标供应商的报价不得超过项目预算金额。

4.投标供应商的报价，应当是本项目采购范围和采购文件及合同条款上所列的各项内容中所述的全部，不得以任何理由予以重复。

5.投标供应商应充分了解项目的位置、情况及任何其它足以影响投标报价的情况，任何因忽视或误解项目情况而导致的索赔将不获批准。

6.投标供应商不得期望通过索赔等方式获取补偿，否则，除可能遭到拒绝外，还可能将被作为不良行为记录在案，并可能影响其以后参加采购方的项目投标。各投标供应商在报价时，应充分考虑报价的风险。

## **付款方式**

1.本项目分两次付款，合同签订及预算下达后支付60%合同款，剩余40%于2021年底项目验收通过后支付，付款前乙方提供甲方等额有效发票。

2.本项目投标报价（合同价）是包含招标需求所列所有项目，投标人不得以任何理由要求采购方支付其他费用。

## **实质性响应条款偏离表**

|  |  |
| --- | --- |
| 序号 | 具体内容 |
| 1 | 服务期限：2021年全年。 |
| 2 | 付款方式及条件：  1.财政预算下达后付款。  2.合同签订且乙方提供合乎甲方要求、等额有效发票后15个工作日内，甲方向乙方支付60%合同款。  3.2021年底验收，验收合格后支付合同余款；乙方提供合乎甲方要求、等额的发票并提交书面服务承诺验收通过后支付。验收后剩余的服务期限内，乙方必须继续履行合同，完成服务，并做好工作交接。  4.乙方必须做好与之前服务公司的工作交接，如因本项目招标延误或其他原因导致前期服务延期的，乙方应按自然日支付原服务公司支付相应的费用，金额按中标金额中驻点维护和安全服务费用计算。 |

**注：上表所列内容为不可负偏离条款**

## **风险责任**

１.投标人应完全地按照项目招标（采购）文件的要求和投标（应答）文件的承诺完成本项目，出于自身财务、技术、人力等原因导致项目失败的，应承担全部责任。

2.投标人在实施过程中应对自身的安全生产负责，若由投标人原因发生的各种事故采购方不承担任何责任。

3.投标人派出的服务人员，若因从事其他单位事务引起事故和纠纷，应由投标人负责，采购方不承担任何责任。

# **开标、评标和定标**

## （一）开标

1.采购方自行组织开标。开标时所有投标人代表不参加。

2.开标时，由采购方采购小组检查投标文件的密封情况；经确认无误后进行拆封，宣布投标人名称、投标价格和招标文件规定的需要宣布的其他内容。

## **（二）评标**

1.评标方法：本评标办法采用综合评分法。即在最大限度满足招标文件实质性要求前提下，按照招标文件规定的各项因素进行量化打分，以评标总得分最高的投标供应商作为中标供应商的评标方法。

2.评标步骤：

（1）资格性审查：开标结束后，评标人员应当依法对投标人的资格进行审查，未通过资格性审查的投标人，不进入符合性审查。

（2）符合性审查：评标人员应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。未通过符合性审查的投标人，不进入技术、商务和价格评审。

（3）详细评审及推荐中标候选人：

①评标人员对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价，具体技术、商务、价格部分的评审因素详见《综合评分表》。

②评标过程中，不得去掉报价中的最高报价和最低报价。

③综合得分=技术得分+商务得分+价格得分。

③使用综合评分法的采购项目，评审得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，由采购小组采取随机抽取方式确定。

## **（三）定标**

1.采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。

2.按照最高得分的定标方法进行定标。

3.评标人员提交评审报告及采购结果，并在馆内公示3日。不在中标名单之列者即为未中标人，采购方不再以其他方式另行通知。

4.中标人拒绝与采购方签订合同的，采购方可以按照招标文件规定的定标原则，重新确定中标人，也可以重新开展政府采购活动。

**综合评分表**

| **序号** | **评分因素** | **分值** | **评价内容** |
| --- | --- | --- | --- |
| 一 | 投标报价（20分） | 20 | 得分按以下公式计算：得分=Z/Sn×20  其中：Z----通过资格性审查和符合性审查且报价不超过预算控制金额的最低投标报价。  Sn----通过资格性审查和符合性审查且报价不超过预算控制金额的投标报价。 |
| 二 | 技术部分  （40分） | 15 | **1.整体方案：**投标人制定项目运维实施方案，专家根据实施方案内容的完整性及满足技术服务需求的情况进行横向比较，分档评分：评价为优得15分（方案优秀无负偏离）；评价为良得10分（方案合理无负偏离）；评价为中得5分；评价为差得0分；用户需求偏离表负偏离一项扣5分，扣完为止。 |
| 15 | 1. **服务质量情况：**   （1）IT维保和信息安全服务：投标人具有在同一党政机关实施的连续期限满5年信息安全服务或IT维保服务案例的，得1分，每增加3年的加1分；以此类推，最高得5分。注：提供合同及续签合同（补充协议）关键页（含签订合同双方的单位名称、合同项目名称、项目金额与含签订合同双方的落款盖章、签订日期的关键页）复印件加盖投标人公章，未提供证明材料的不得分。  （2）投标人所签约的信息安全服务甲方单位近五年内在副省级或以上城市党政机关信息安全的总体情况通报文件中被通报表扬的，每提供一个受表扬单位案例得1分，最高得10分。  注：提供副省级或以上城市党政机关信息安全情况的通报文件以及与被表扬单位签订的服务合同关键信息页扫描件，原件备查，未按要求提供或提供不清晰导致专家无法判断的不得分。 |
| 10 | **3.项目拟使用的工具情况：**投标人具备开展业务信息系统服务器漏洞扫描、网络层扫描、移动安全漏洞扫描及对外服务网站应用层扫描所使用的专业检测工具，能提供5种及以上不同工具得10分，提供4种工具得7分，提供3种工具得4分，提供2种及以下工具得1分,无专业扫描检测工具，不得分。  （1）自行开发的专业工具软件，提供《软件著作权登记证书》扫描件。  （2）投标人采购的专业工具软件，要求提供检查工具品牌、型号、与工具厂商签订的合同证明资料复印件，原件备查。提供的证明文件不满足要求或未提供证明文件的不得分。 |
| 三 | 商务部分（40分） | 10 | **1.投标人资质情况：**  （1）具有国家高新技术企业证书得2分，无则得0分；  （2）具有国家测评中心颁发的信息安全风险评估服务资质证书的得2,无则得0分；  （3）具有国家网络安全审查技术与认证中心信息安全应急处理服务资质证书得2,无则得0分；  （4）投标人具有保密技术防护专用系统研制资格得2分,无则得0分；  （5）投标人是网络安全威胁信息共享平台合作支撑单位的得2分，无则得0分。  **注：**第（1）（2）（3）点提供有效期内的相关证书复印件；第（4）提供保密局出具保密技术防护专用系统研制资格的批文扫描件；第（5）点可通过资质授予方官方渠道查询。  提供有效期内的相关证书复印件或扫描件并加盖投标单位公章；原件备查，不提供，不得分。 |
| 10 | **2.拟安排的项目负责人情况**：投标人拟安排的项目负责人必须为投标人自有员工，具有学士或以上学历，同时具有以下工作经历及技术资格证书：  （1）项目负责人有参与承担制定国家信息安全技术类标准课题研究的，得2分；  （2）项目负责人具有高级网络安全工程师证书、信息系统高级项目管理师证书、CISP证书、PMP证书，每个证书得2分，该项最高得8分  注：提供学位证书、技术资格证书或相关证明文件的扫描件，原件备查，未按要求提供或提供不清晰导致专家无法判断的不得分。 |
| 10 | **3.安排的项目团队成员情况（项目负责人除外）：**  投标人须承诺拟安排人员为本单位正式员工，须承诺项目团队成员不少于7人，2名技术人员驻场办公，不承诺此项不得分（提供驻场承诺书加盖公章)；如有虚假，将做投标无效处理，涉嫌存在违法违规行为的，依法报主管部门处理处罚。在此基础上，按以下标准评分：  （1）1名驻场工程师同时具有ISO/IEC-27001证书、华为云HCNA证书得2分；  （2）1名驻场工程师同时具有CCNP证书、RHCE证书得2分；  （3）1名安全专家同时具有高级项目经理认证资格证书、CISP证书、CISAW证书的得2分；  （4）其他项目团队成员4名，具有CISAW或CISP证书的，每一人得1分，最高得4分。  **注：**提供团队人员技术认证证书复印件或扫描件加盖投标人公章（原件备查）。提供的材料不满足要求的不得分。 |
| 5 | **4.投标人业绩情况：**2018年1月1日至投标截止日（以合同签订日期为准），投标人承担过类似项目经验的（单个项目服务期不低于一年）：每提供一个得1分，最高得5分。同一项目不重复计分。  注：提供体现合同甲乙方、合同时间、服务期限、金额、服务类内容等的合同关键页或中标通知书扫描件。不提供或者不能有效证明的，不得分。 |
| 2 | **5.获奖情况：**  投标人最近两年参加省级及以上网络安全应急演练比赛，获奖一次的得1分，连续两年获奖的得2分。  （提供获奖的证明文件扫描件,未提供或不清晰无法判断的不得分）。 |
| 3 | **6.服务网点：**（1）深圳供应商，或非深圳供应商但在深圳有合法注册的分公司（或服务机构）（分公司的必须提供分公司营业执照扫描件，服务机构必须同时提供服务合作合同及服务机构营业执照扫描件作为得分依据，原件备查）的，得3分；否则不得分。  （2）本地无服务机构的外地供应商承诺：中标后两周内设立本地经营（服务）网点的，提供加盖公司印章承诺文件（格式自定）的，得2分；未提供承诺或承诺内容不满足要求均不得分。 |

# **投标文件**

**投标人提供投标文件一份正本三份副本，投标文件由以下部分组成：**

1. 目录
2. 投标函
3. 履约承诺函
4. 投标人情况介绍
5. 报价一览表
6. 投标人资格证明文件（非原件必须加盖公章）包括但不限于以下文件：

1.营业执照或事业单位法人证（复印件或扫描件）；

2.法定代表人证明书原件；

3.法定代表人授权委托证明书原件（法人投标时无须提供）；

4.近三年内（投标人成立不足三年的可从成立之日起算）无重大违法犯罪记录和不存在处于被禁止参与政府采购活动期限内情形的书面声明；

5.未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，投标文件中提供证明材料；

（通过“信用中国”网站(www.creditchina.gov.cn)、深圳政府采购监管网(zfcg.sz.gov.cn)、深圳信用网（www.szcredit.org.cn）等渠道查询的相关主体信用记录，必须提供每个网站查询的所有记录；)

6.**《信息安全服务资质安全工程类》证书或《信息安全服务资质认证》证书**，及其他本项目涉及的公司资质证明文件；

7.本项目不接受联合体投标，不允许分包、转包（投标人提供声明函，格式自拟）；

8.投标人需要提供的其他证明文件。

注：投标人提供的以上资料若为复印件或扫描件的需加盖公章。

1. 实质性响应偏离表
2. 用户需求偏离表（格式自拟）
3. 详细分项报价（格式自拟）
4. 项目分析报告及人员配置和管理方案（提供人员资质证明，格式自拟）
5. 实施方案（格式自拟）
6. 项目的服务承诺（格式自拟）
7. 违约承诺及项目服务期满后的服务承诺（格式自拟）
8. 响应时限（格式自拟）
9. 项目安全保密及保障措施（格式自拟）
10. 投标人过往服务质量和业绩证明文件
11. 项目涉及或投标人认为需要加以说明的其他内容

# **其他要求**

（一）中标人应在进驻前必须提交详细的服务方案和计划，其中应包含本项目所要求的所有服务，和服务团队人员资料（须包括身份和资质证明）。服务团体组成人员资质及数量情况不得低于投标文件所述。

（二）中标人应与采购方签署保密协议，对工作中接触的所有资料信息保密。

（三）投标人使用的标准必须是国际公认或国家、或地方政府颁布的同等或更高的标准，如投标人使用的标准低于上述标准,评标委员会将有权不予接受，投标人必须列表将明显的差异详说明。