第二章 需求一览表及需求明细

第一节 需求一览表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **数量** | **单位** |
| 1 | 深圳市投资推广署信息安全服务项目 | 1 | 项 |

**特别说明：**

1、本招标文件仅适用于本次招标公告中所叙述的项目。

2、投标人可根据各自公司的经营范围对本“招标文件”中“采购项目”所列的所有采购内容进行投标，但不得将项目中的内容拆开投标，否则将导致其投标被拒绝。投标人须认真填写第五章的偏离表，偏离表将作为重要的评标依据。

3、投标人应在投标文件中标明页码及索引，以便于评标委员会的查阅。

4、投标人有义务在招标活动期间浏览深圳国际招标采购网（http://[www.sztc.com](http://www.ymcw.com)）和深圳政府采购网（http://www.cgzx.sz.gov.cn，招标机构在网上公布的与本次招标项目有关的信息视为已送达各投标人。

 第二节 商务需求明细

**一、服务期限**

自签订合同之日起提供累计满一年服务。

**二、售后服务期限**

服务期满后，应继续提供服务至下一年度招投标工作启动前。

**三、验收要求**

主要项目成果及服务需获得采购单位认可，并通过专家评审。

第三节 技术需求明细

**一、项目背景**

为了规范我署信息安全管理体系框架，落实各项网络安全工作，提高单位人员信息安全意识，加强基础信息网络和重要信息系统的安全防护能力和水平，保障网络和信息系统安全、稳定地运行，依据我国信息安全等级保护制度的相关规定，结合上级单位关于深圳市党政机关信息安全联合检查要求，组织开展安全制度落实、技术防护和安全保障等各项工作，认真查找安全隐患和漏洞，完善各项防护措施，全面提高我署信息安全风险管理水平。

**二、具体技术要求**

1、编制计划和方案

根据《2018年深圳市党政机关信息安全联合检查工作方案》文件要求编写采购人本年度信息安全保障工作的计划和实施方案。

2、安全管理完善

按照《2018年深圳市党政机关信息安全联合检查工作方案》要求，根据采购人现状修订信息安全管理机构和制度。指定信息安全主管领导和各职能负责人，并签署相关责任文件和保密文件，同时根据已有的信息安全制度保存相关实施的记录。

3、安全漏洞扫描

每季度配合采购人完成用户终端及托管于资源中心的服务器、信息系统的安全漏洞扫描漏洞整改工作。交付物包括但不限于《服务器扫描计划》、《服务器漏洞扫描结果报告》、《网站应用层漏洞扫描扫描计划》、《网站应用层漏洞扫描扫描结果报告》、《计算机终端漏洞扫描结果报告》。

4、安全事件监控

为了进一步加强采购人的信息防护能力，减免信息安全事件的发生概率，要求中标方定期确认是否下发新一期计算机终端信息安全周报，并配合采购人处理存在信息安全风险的终端；配合采购人每半年一次对网站进行密件及携带病毒文件的查杀工作。交付物包括但不限于《终端安全事件处理记录》、《对外网站暗链、后门、密件及病毒文件查找记录》。

5、渗透测试

每季度一次对采购人所有信息系统开展渗透测试检查工作，以黑客角度手工方式挖掘漏洞，通过该项工作进一步摸清应用系统及网站的安全性，避免出现信息安全事件。渗透测试过程发现的安全漏洞将汇编至《渗透测试报告》。

6、风险评估

对采购人已上报的信息系统每年一次开展风险评估工作, 通过开展信息安全风险评估工作，摸清用户方信息系统的安全风险状况，对发现在的不可接受的风险进行整改和实行有效的控制。提高基础信息网络和重要信息系统的安全防护能力，增强信息安全意识，促进信息化建设稳定持续的发展。

7、信息安全等保测评工作

中标方应协助完成对采购人2个已备案信息系统进行等级保护测评，协助第三方测评机构出具《等级保护测评报告》，并对发现的安全隐患配合采购人进行整改。

8、网络与信息安全突发事件应急响应

提供7x24小网络与安全事件的应急响应工作，应急响应主要针对突发的网站安全故障、网络安全事件、应用系统安全事件、主机安全事件、黑客攻击事件等进行诊断、分析并协助解决。在完成应急事件响应处理后的3个工作日内向采购人供事件的处理记录及问题整改建议。

9、网站7\*24小时监控

为采购人所有对外网站提供7X24小时的网站安全监控服务，监控服务要求如下：

9.1网站安全监控服务应支持实时对网站暗链扫描和挂马检测，要求采用与市经贸信息委（市信息安全测评中心）所用的安全绩效考核监控平台品牌型号及版本一致；

9.2监控平台需支持7X24小时对网站可用性监控，支持检测和监控网站首页响应速度，判断网站是否掉线；

9.3在发现安全问题后，需在半小时内以短信、电话和邮件等多种方式告知我委；

交付物：《网站监控周报》。

10、安全培训

要求中标单位每年对采购人开展一次全员信息安全意识教育，培养工作人员的信息安全意识，提高其信息安全知识水平，以更好地为信息安全建设和管理工作服务。

11、安全咨询

在信息安全措施、安全策略、安全问题、安全管理体系等方面为采购人提供信息安全技术咨询服务。

12、年度迎检工作配合

配合采购人完成《2018年深圳市党政机关信息安全联合检查指标及评分标准》各项要求的自查和整改工作，并在10月底前完成包含各项汇报材料，取证截图及相关制度执行记录、培训记录等的《年度信息安全联合检查迎检资料汇编》。

13、上网行为审计服务

提供上网行为审计服务一年，满足以下要求：100M带宽/1000人以下网络环境使用；最大并发连接数为70万，最大新建连接数为24000/秒；

1U硬件，标配6个千兆电接口（其中含1个管理接口和1个HA接口），2个扩展槽（可选配扩展网卡），128G SSD硬盘，单交流电源。

**三、具体工作要求**

**1、信息资产统计**

帮助采购人对现有信息资产进行梳理和登记造册，范围包括但不限于终端电脑、服务器、网络及安全设备，登记内容应至少包括资产的类型、版本、IP地址、使用状况等。

**2、日常办公电脑问题处理**

负责采购人办公电脑终端软硬件故障排查及办公软件的安装工作，必要时对原厂保修期内的硬件设备代为联络维修，跟踪维修情况。

**3、周边设备维护**

提供对打印机、扫描仪等电脑外接设备的安装配置、跳线链接等非硬件相关（如硬件故障、碳粉或硒鼓更换等）的维护服务。

**4、网络维护**

负责采购人网络通信线路的维护保障、局部环境的网络接线、楼层机房的网络设备维护、网络模块更换等工作。对各接入点的链路故障及异常，需要及时排查、诊断、解决故障，保障网络可靠性，并针对故障原因提交故障分析报告。

**5、软硬件产品代购服务**

提供软硬件产品代购服务，若采购人有紧急使用设备或更换设备配件的需求且代购产品采购价格不超过伍仟元人民币，采购人有权要求中标方先行垫付采购，再按照采购人报销进行结算。若代产品采购费用超过伍仟元人民币，采购人将与中标方进行协商处理。

**6、信息化规划咨询**

为采购人提供对如网络规划、信息系统规划等信息化相关问题提供技术咨询。

**7、现有信息系统使用支持**

要求中标方驻场人员熟练使用采购人现有信息系统，根据采购人实际需求配合相关工作人员进行日常事务处置和信息系统的维护工作。

**8、其他服务内容**

完成采购人安排的其他相关工作。

**9、驻场要求**

提供一名5 X 8小时3年以上工作经验的驻场人员，保障日常信息化运维服务。中标方有义务保证驻场人员能胜任本项目运维工作，若驻场人员不满足招标方要求，采购人有权要求更换。且驻场人员一旦被招标方确认，将固定在采购人长驻服务，直到服务合同结束为止。