招标项目需求

一、对通用条款的补充内容

|  |  |  |
| --- | --- | --- |
| **序号** | **内 容** | **规 定** |
| 1 | 联合体投标 | 见《招标公告》中“投标人资格要求”部分的相关内容 |
| 2 | 投标有效期 | 120日历天（从投标截止之日算起） |
| 3 | 投标人的替代方案 | 不允许 |
| 4 | 投标文件的投递 | 本项目实行网下投标，按照谈判文件的要求提交纸质文件正本1份、副本4份、电子文件1份，所有谈判应答文件应于递交截止时间之前送达谈判文件规定的地址。 |
| 5 | 履约保证金 | \_\_\_\_\_万元或合同金额的\_\_\_\_\_%，缴纳方式： |
| 6 | 中标服务费 | 根据“深圳市财政委员会关于规范深圳市社会采购代理机构管理有关事项的补充通知(深财购[2018]27号)”的规定执行。招标代理服务收费以中标/成交通知书公布的中标金额为计算基准,按差额定率累进法计算,招标代理服务费不足伍仟按伍仟收取。 |

备注：本表为通用条款相关内容的补充和明确，如与通用条款相冲突的以本表为准。

二、实质性条款

|  |  |
| --- | --- |
| 序号 | 具体内容 |
| 1 | 完全满足本项目服务期限的要求。 |
| 2 |  |
| …… |  |

注：上表所列内容为不可负偏离条款

三、项目概况

（一）预算金额: 人民币383,400.00元，最高投标限价: 人民币383,400.00元

（二）项目概况:

根据深圳市党政机关信息安全联合检查工作要求，为做好我局2021年度网络与信息安全工作，根据有关规定，开展信息安全管理体系、信息安全管理制度、信息安全风险评估、信息安全等级保护、信息安全防护、应急体系建设、安全教育培训、安全隐患排查及整改等信息安全服务工作。

四、项目技术要求

**1.服务资产范围**

服务器及相关信息系统资产数量表

| 序号 | 设备名称/型号 | 数量 |
| --- | --- | --- |
| 1 | 服务器及存储设备 | ≥30台 |
| 2 | 交换机、路由器等主要网络设备 | ≥36台 |
| 3 | 安全设备 | ≥30台 |
| 4 | 应用系统 | ≥13套 |
| 5 | 外网终端 | ≥400台 |
| 6 | 内网终端 | ≥400台 |

**2.服务需求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 工作内容 | 服务项目 | 服务要求 | 全年服务次数 |
| 1 | 信息安全制度制定与落实 | （1）信息安全制度制定、优化及落实 | 梳理和核查包括不限于以下各项信息安全管理制度及制度执行情况：  a）信息安全管理机构成立情况；  b）信息安全管理职能部门设置；  c) 信息安全管理人员配备；  d) 信息系统的规划、建设、运维、废弃等环节的信息安全制度制定；  e) 信息安全制度执行情况记录。 | 1次 |
| （2）信息安全管理体系落地 | a）建立适合我方实际的信息安全管理体系框架；  b）评估和识别关键的业务处理流程、资产和岗位设置等；  c) 实现安全体系文档化，管理流程化、绩效控制可量化和安全意识普及； | 1次 |
| 2 | 个人信息和重要数据保护 | / | 针对用户单位信息系统情况，按照《信息安全技术个人信息安全规范》规定，完成用户单位个人信息和重要数据在组织管理、制度建设、人员管理、技术保障、规范操作等方面的工作。 | / |
| 3 | 信息安全风险评估 | （1）资产识别 | 1、根据资产、业务流程的特性和重要程度对资产进行科学的分类（数据、服务、声誉、硬件和软件、通讯、程序界面、物理资产、支持设施、人员和访问控制措施等有形和无形资产），并参考CIA（保密性、完整性和可用性）进行价值分级和定量，以识别关键的信息资产。  2、收集统计用户单位在使用的计算机资产下列信息，包含：  a）计算机主机名；  b）计算机IP地址；  c）计算机MAC地址；  d）计算机使用人或责任人；  e）计算机所属部门；  f）计算机的物理位置；  g）服务器的内外网IP对应。 | 1次 |
| （2）威胁识别 | 通过安全策略检查、文档查看、业务流程分析、网络拓扑分析、人员访谈、入侵检测系统收集的信息和人工分析等手段对可能潜在的威胁进行分类、分析和定性。 | 1次 |
| （3）脆弱性识别 | 以资产为核心，针对每一项需要保护的资产、识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估，分析出有可能被潜在威胁源利用的系统缺陷或脆弱性列表，并对其进行分级。 | 1次 |
| （4）现有控制措施有有效性 | 结合资产、威胁和脆弱性分析结果，对现有的预防性安全措施和保护性安全措施进行有效性测试、评估。 | 1次 |
| （5）风险分析 | 资产-威胁-脆弱性映射关系以及控制措施效果，分析存在的安全风险发生的可能性和影响。 | 1次 |
| （6）风险计算 | 以关键业务系统为关联要素，通过资产的价值、资产面临的威胁和存在的脆弱性三个方面的内容进行量化，统计分析风险值，评定业务系统所属的风险范围和等级。 | 1次 |
| （7）风险结果 | 通过层面汇总分析和综合分析等过程找出信息系统的安全风险，识别影响系统安全保护能力的安全隐患，形成评估结论报告。 | 1次 |
| （8）风险处置方案 | 针对信息安全风险评估结果和存在的关键性问题，提出相应的不可接受风险处置建议和方案。 | 1次 |
| 4 | 信息安全等级保护 | （1）等级保护备案 | 尚未定级备案信息系统提供协助等级划分、定级和协助用户单位做好备案工作。 | 根据用户单位需求 |
| （2）协助等级保护测评 | 协助测评单位对用户单位等级保护一级以上信息系统开展信息系统等级保护测评工作。 | 根据用户单位需求 |
| 5 | 安全防护措施落实 | （1）防病毒 | 协助检查内外网计算机的病毒特征库是否更新至最新。 | 4次 |
| （2）系统补丁升级 | 根据实际情况，对用户单位所有windows服务器和终端进行补丁更新升级维护 | 4次 |
| （3）商用邮箱检查 | 协助用户单位是否使用商用邮箱开展检查工作，检查在网站中是否使用商用邮箱 | 4次 |
| （4）非法外联 | 协助检查内网终端是否存在违规连接互联网的情况。 | 根据实际情况 |
| （5）弱口令检查 | 检查所有终端、服务器、网络安全设备等是否存在弱口令。 | 4次 |
| （6）敏感信息检查 | 检查门户网站和其他对外发布的网站中是否存在敏感信息、非法言论等。 | 4次 |
| （7）安全策略优化 | 基于用户单位现有的安全设备，根据实际情况，对安全策略的策略进行优化 | 根据实际情况 |
| （8）安全设备巡检 | 每月对用户单位所有在运行的安全设备进行安全巡检，做好巡检记录。 | 4次 |
| （9）终端安全保密自查 | 对用户单位所有终端提供技术支持，协调完成终端安全保密自查工作 | 2次 |
| 6 | 安全培训 | （1）安全培训计划 | 根据用户单位信息系统和人员的情况，设置合理的培训课程和培训计划。 | 1次 |
| （2）安全意识培训 | 主要培训办公电脑、平板、智能设备、移动存储设备等终端设备在使用互联网、内网网络的安全、保密意识和安全常识。 | 1次（培训时间不少于2个小时） |
| （3）等级保护标准  培训 | 主要培训国家等级保护工作政策、行业标准、监管要求、最佳实践等方面的发展情况。 | 1次（培训时间不少于2个小时） |
| 7 | 安全隐患排查与整改 | （1）主机层扫描 | 针对服务资产范围中的服务器、网络设备、安全设备等资产进行主机层扫描，发现存在的漏洞并给出修复建议。 | 4次 |
| （2）风险整改 | 针对上期党政机关信息安全联合检查风险评估中发现的不可接受风险，给出修复建议，协助进行安全整改和加固，最大程度消除安全隐患。 | 1次 |
| （3）信息安全联合检查整改 | 完成上年度信息安全联合检查的整改工作。 | 1次 |
| （4）新系统上线前安全检测 | 对用户单位新系统网络层和应用层进行上线前安全检测，发现存在的漏洞并给出修复建议。 | 根据实际需求 |
| 8 | 信息安全通报 | 定期通报安全行业动态、系统漏洞和病毒预警信息，通过电子邮件形式发送给用户单位信息安全管理员。 | 行业动态通报：  对信息安全领域的动态进行通报。 | 12次 |
| 漏洞安全通报：  对新出现的安全漏洞进行通报。 | 12次 |
| 病毒安全通报：  对新出现的较严重病毒进行通报。 | 12次 |
| 针对安全通报的内容，对用户单位的安全现状进行自查和整改 | 根据实际情况 |
| 9 | 内设机构及直属单位信息安全工作 | （1）检查方案 | 协助用户单位制定内设机构及直属单位信息安全检查工作方案。 | 按用户要求 |
| （2）检查实施 | 为用户单位对内设机构及直属单位信息安全现场检查过程中提供相关技术支持。 | 根据实际情况 |
| （3）检查总结 | 协助用户单位编写全年内设机构及直属单位信息安全工作总结。 | 1次 |
| 10 | 信息安全防护 | （1）服务器安全防护 | 定期对服务器进行安全检测并做出分析报告。按市“信息安全”指标考评要求，协助用户单位完成检测、漏洞修复及结果上报工作。 | 4次 |
| （2）网站安全防护 | 定期对公众服务网站系统进行安全检测并做出分析报告。按市“信息安全”指标考评要求，协助用户单位完成检测、漏洞修复及结果上报工作。 | 4次 |
| （3）信息系统安全防护 | 定期对信息系统进行安全检测并做出分析报告。按市“信息安全”指标考评要求，协助用户单位完成检测、漏洞修复及结果上报工作。 | 4次 |
| （4）终端安全防护 | 定期对终端电脑进行安全检测并做出分析报告。按市“信息安全”指标考评要求，协助用户单位完成检测、漏洞修复及结果上报工作。 | 4次 |
| 11 | 联合检查与绩效评估自查与总结 | （1）自查与整改 | 按照深圳市信息安全主管部门相关文件要求协助用户单位完成2021年信息安全联合检查和绩效评估差距分析和整改。 | 1次 |
| （2）材料汇编 | 按照上级相关文件要求协助用户单位编制2021年信息安全检查相关材料。 | 1次 |
| 12 | 应急响应支持 | 应急响应及处置 | 当用户单位内网、外网及其主机系统发现有安全问题时，需立即安排资深安全维护工程师前往事发现场，查明发生问题的原因，采取有效的措施，尽快恢复网络和主机的正常运行。一般问题应急处置人员应在2小时内到达现场，重大问题应在1小时内到达现场。  每次安全问题处理后，应保存现场所有处置资料，分析问题产生的原因，记录维护使用的方法、步骤和参数，制定防止类似问题再次发生的解决方案，并将保存的现场资料和有关文档资料提交给用户单位。 | / |
| 应急响应值守 | 当遇到国家法定节假日、国家事件和重大会议、上级单位特殊要求等期间，需安排人员实行7\*24小时应急值守，如遇到信息安全突发事件，应协调组织安全专家团队及时赶赴现场提供应急响应服务,做到及时发现、及时处理高效工作机制。 | / |
| 13 | 市主管部门工作要求 | / | 根据市信息安全主管单位的政策、文件要求，积极开展各项信息安全自查、技术防护措施和安全整改等工作，并将工作完成情况及时向相关主管部门回函。 | 根据实际情况 |
| 14 | 顾问咨询 | / | 供安全咨询支持，担任网络安全的咨询顾问，在网络、主机和信息系统进行升级、扩建时，提供安全顾问咨询服务，和信息安全评估服务，并根据实际情况提供咨询服务解决方案等。  作为咨询顾问，需要提供全方位的咨询服务，通过电话、E-mail、现场研讨等方式，协助对信息系统中出现的安全问题或与安全相关的问题进行处理。 | 根据实际情况 |

**具体服务技术要求（补充上表）**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务内容** | **技术要求** |
| **1** | **信息安全风险评估** | （1）风险评估范围覆盖用户单位所有信息系统； |
| （2）进行风险评估必须具有中国信息安全认证中心或中国信息安全测评中心等权威机构颁发的相关资质证书、进行风险评估的第三方人员必须具有的资质指取得权威机构颁发的认证证书，如：CISAW、CISP、CISSP等证书。 |
| （3）对内网、外网网络、主机服务器及所有客户端电脑进行安全风险分析；对所有主机服务器的端口、配置进行的安全检查、对操作系统级和数据库级的系统安全漏洞进行安全处理； |
| （4）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用户单位； |
| （5）担任用户单位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。 |
| （6）为用户单位提供不限次数的信息系统应急响应服务。 |
| **2** | **安全培训** | 要求有完善的培训与讲座实施计划；信息安全全员讲座由中标供应商安排曾经承担过政府机构相关讲座经验的专家承担；中标供应商应提供配套PPT、书面教材，由不低于国家测评中心CISP资格的讲师承担。 |

**3.服务要求**

**3.1.人员要求**

（1）人数：中标方必须为本项目成立本地化服务小组,派驻本项目的实施技术人员和项目经理必须固定，如有变更，必须经用户同意确认，中标供应商组建不少7人的项目实施技术服务团队，其中1人为项目经理。

（2）对项目经理要求：具有至少五年与本项目类似的安全服务工作经验并担当服务经理，具有相关技术资格证书。

（3）需常备1名机动安全专家，以便于在紧急情况或工作量较大时，可随时抽调熟悉相关环境的工程师进行补充。机动安全专家具有相关技术资格证书。

（4）中标方应安排参与本项目的服务人员至少有7人，提供2名安全工程师驻场服务，驻场工程师具有CISP或项目经理证书，在突发应急事件或工作量大时，能临时增加2名技术服务人员。

（5）未经过招标单位同意，中标方不得变换项目实施团队人员。如有变更，必须经用户同意确认，项目经理或主管具有一定的技术及管理知识和经验，能够容易地与客户沟通，能够很好地执行并完成服务工作，并能根据一些特殊的情况可以适当增加服务人员，接受用户与单位的统一管理。

**3.2.技术要求**

（1）编写项目总体安全服务方案，对各项工作的内容、方法、时间进行描述，其中工作时间要以周为单位进行量化；

（2）每月一次例行阶段工作总结，详细描述各项工作的开展情况、当前进度、取得的成果、预期完成时间、发现的问题并书面呈报，同时准备会议材料；

（3）对在项目实施中需要协调和协助的工作，需至少提前一周书面通知相关岗位人员，以便有充分的时间安排时间和业务协调；

（4）项目实施中所有的文档：过程数据、会议纪要、过程文档、计划、方案、策略等，必须以电子、纸制同时保存（至少一式两份存档），随时接受检查；

（5）针对不同的工作内容实行文档（电子及纸制）分类管理，文档分类要清晰，能做到按天、按周、按月进行检索，容易调阅。每项工作完成后都必须有相应的工作附件与之呼应；

（6）项目实施中对信息系统采用的任何技术检测（本地核查、网络扫描、安全分析、设备调研）手段和方法，必须事先提交详细的实施（检测）方案，明确检测内容、方法、使用的规则（策略）、可能引发的后果、以及后果的处理等内容，经确认通过后方可进行实施；

（7）所有对数据库系统和应用系统的技术测试必须预选制定数据备份和恢复方案，并提交相关岗位工程师确认。在方案获得确认后，先对目标系统进行备份并验证备份数据的有效性，确认备份数据有效后再进行相关技术测试（相关技术测试必须事先提交过测试方案并获得用户单位确认后方可实施）；

（8）按时完成本年度信息安全联合检查工作各阶段要求的上报材料（如工作计划、实施方案、核查表等）并准时提交；

（9）为保证用户单位信息系统安全，所有有关项目的文档，无论电子还是纸质均不可带出项目现场。

**3.3.应急响应要求**

（1）将提供7\*24小时服务，在发生故障需要提供技术支持时，保证能够联系上相关服务人员。

（2）在出现紧急事件时，接到报告后，以最快的速度（1小时内）派遣安全技术工程师到达现场，协助进行处理，技术支持人员在解决故障时，要最大限度保护好数据，做好故障恢复的文档，力争恢复到故障点前的业务状态。对于“系统瘫痪，业务系统不能运转”的故障级别，如果不能于12小时内解决故障，必须16小时内提出应急方案，确保业务系统的运行。故障解决后24小时内，提交故障处理报告，说明故障种类、故障原因、故障解决中使用的方法、故障损失、以及优化建议等情况。

**3.4.行为规范要求**

（1）中标方派驻人员需要严格遵守用户单位的规章制度，严格按照用户单位相应的规章制度办事。

（2）中标方与用户单位其他各合作方在协同工作时，需要密切配合，同时要将双方协商的工作方案及时反馈到用户单位负责人员，再确定落实与否。

（3）遵守保密原则。服务过程中所产生所有文档资料和数据均为招标方所有，服务期间或服务期结束后，中标方必须对服务过程中接触的信息系统中所有信息和数据、服务过程中产生的所有信息和数据等进行严格的保密。不得以任何方式向外界传递或泄露任何相关信息或数据，一旦发现，将追究中标方法律责任。

**3.5.服务工具要求**

（1）用于信息安全服务的检测设备由中标供应商负责提供，同时要保证工具的正版化。

（2）投标人响应并承诺提供漏洞扫描检测工具5套。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。

**3.6.服务质量违约要求**

在合同服务期内，出现以下情况的视为安全技术服务质量没有达到要求，将对中标方进行违约罚款，金额从服务合同金额中核减：

（1）因中标方原因导致信息安全工作被采购人上级主管单位点名批评的，每次扣除合同金额1000元。

（2）因中标方工作不到位，导致发生信息安全事件的，每次扣除合同金额5000元。

（3）因中标方未能发现并协助消除安全隐患，或所做工作不到位，导致采购人在市信息安全主管部门检查中扣分的，每扣1分扣除合同金额2000元。

（4）发现中标方技术服务人员在工作时间从事其他与信息安全工作无关的，第1次警告，从第2次起，每次扣除合同金额1000元。

（5）在出现紧急事件时，中标方未达到应急响应要求，未在规定的时间内到达现场或解决故障的，每次扣除合同金额1000元。

（6）中标方发现问题并向采购人提交建议解决方案，但采购人或采购人委托的技术开发方不处理或处理不到位导致信息安全检查被扣分，中标方不承担责任。

五、项目商务要求

（一）服务期限：一年，自合同签订之日起计算。

（二）合同方式：固定总价合同，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。由企业根据招标文件所提供的资料自行测算投标报价；一经中标，投标报价总价作为中标单位与采购人签定的合同金额，合同期限内不做调整。

（三）付款方式：

1、合同签订后支付80%；

2、服务合同到期支付剩余20%（若未出现“服务质量违约要求”的可按要求支付剩余合同款20%，若出现“服务质量违约要求”的按实际情况扣除相应合同款后支付剩余款项）。

（三）质量考核验收标准及违约金

质量考核验收标准：

1、在现场检查前完成所有的联合检查工作，并移交项目中的电子和纸制过程文档；

2、在材料上报的各阶段准时完成所有联合检查材料的上报；

3、风险评估结果有效，风险评估报告满足党政机关信息安全联合检查相关要求，顺利通过检查；

4、信息系统定级报告符合要求，并通过公安部门备案；

5、协助第三方测评机构完成用户单位级信息系统的等级保护测评；

6、信息安全管理制度齐全有效，内容可操作性强，并满足党政机关信息安全联合检查的相关要求。

六、投标报价

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。由企业根据招标文件所提供的资料自行测算投标报价；一经中标，投标报价总价作为中标单位与采购人签定的合同金额，合同期限内不做调整。

2.投标人应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；评标时，评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

3.投标人的投标报价，应是本项目招标范围和招标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，并以投标人在投标文件中提出的综合单价或总价为依据。

4.除非政府集中采购机构通过修改招标文件予以更正，否则，投标人应毫无例外地按招标文件所列的清单中项目和数量填报综合单价或总价。投标人未填综合单价或总价的项目，在实施后，将不得以支付，并视作该项费用已包括在其它有价款的综合单价或总价内。

5.投标人应充分了解项目的位置、情况、道路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或服务期限延长申请将不获批准。

6.投标人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政府采购的项目投标。各投标人在投标报价时，应充分考虑投标报价的风险。