**附件1 法定代表人（负责人）资格证明书**

**法定代表人（负责人）资格证明书**

同志，现任我单位 职务，为法定代表人**（负责人）**，特此证明。

有效日期：

签发日期：

 投标单位名称（单位盖公章）：

 法定代表人（签字或盖章）：

说明：

1.法定代表人为企业事业单位、国家机关、社会团体的主要负责人。

 2.内容必须填写真实、清楚，涂改无效。

注：要求必须提供法定代表人（负责人）身份证复印件（正反两面）。

**附件2 法定代表人授权委托书**

**法定代表人授权委托书**

本授权委托书声明：我（姓名）系（投标供应商名称）的法定代表人（负责人），现授权委托（姓名）为我公司签署 项目已递交的投标文件的法定代表人（负责人）的授权委托代理人，代理人全权代表我所签署的本项目已递交的投标文件内容我均承认。

代理人无转委托权，特此委托。

授权单位（单位盖公章）：

法定代表人（签字或盖章）：

签发日期：

有效期至：

附：代理人：

联系电话： 手机：

身份证号码： 职务：

注：要求必须提供代理人身份证复印件（正反两面）。

**附件3 政府采购投标及履约承诺函**

**政府采购投标及履约承诺函**

致：深圳市龙岗区卫生监督所

我单位承诺：

1.我单位关于本招标项目所提供的货物或服务未侵犯知识产权。

2.我单位参与本项目投标前三年内，在经营活动中没有重大违法记录。

3.我单位参与本项目政府采购活动时不存在被有关部门禁止参与政府采购活动且在有效期内的情况。

4.我单位具备《中华人民共和国政府采购法》第二十二条第一款规定的六项条件。

5.我单位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

6.我单位参与该项目投标，严格遵守政府采购相关法律，投标做到诚实，不造假，不围标、串标、陪标。我单位已清楚，如违反上述要求，其投标将作无效处理，被列入不良记录名单并在网上曝光，同时将被提请政府采购监督管理部门给予一定年限内禁止参与政府采购活动或其他处罚。

7.我单位如果中标，做到守信，不偷工减料，依照本项目招标文件需求内容、签署的采购合同及本公司在投标中所作的一切承诺履约。项目验收达到全部指标合格，力争优良。

8.我单位承诺本项目的报价不低于我单位的成本价，否则，我单位清楚将面临投标无效的风险；我单位承诺不恶意低价谋取中标；我单位对本项目的报价负责，中标后将严格按照本项目招标文件需求、签署的采购合同及我单位在投标中所作的全部承诺履行。我单位清楚，若我单位以“报价太低而无法履约”为理由放弃本项目中标资格时，愿意接受主管部门的处理处罚。若我单位中标本项目，我单位的报价明显低于其他投标单位的报价时，我单位清楚，本项目将成为重点监管、重点验收项目，我单位将按时保质保量完成，并全力配合有关监管、验收工作；若我单位未按上述要求履约，我单位愿意接受主管部门的处理处罚。

9.我单位已认真核实了投标文件的全部内容，所有资料均为真实资料。我单位对投标文件中全部投标资料的真实性负责，如被证实我单位的投标文件中存在虚假资料的，则视为我单位隐瞒真实情况、提供虚假资料，我单位愿意接受主管部门作出的行政处罚。

10.我单位承诺不非法转包、分包。

以上承诺，如有违反，愿依照国家相关法律处理，并承担由此给采购人带来的损失。

投标单位名称（单位盖公章）：

法定代表人或其委托代理人：

联系方式：

日期： 年 月 日

**附件4 政府采购违法行为风险知悉确认书**

**政府采购违法行为风险知悉确认书**

本公司在投标前已充分知悉以下情形为参与政府采购活动时的重大风险事项，并承诺已对下述风险提示事项重点排查，做到严谨、诚信、依法依规参与政府采购活动。

**一、本公司已充分知悉“隐瞒真实情况，提供虚假资料”的法定情形，相关情形包括但不限于**：

（一）通过转让或者租借等方式从其他单位获取资格或者资质证书投标的。

（二）由其他单位或者其他单位负责人在投标供应商编制的投标文件上加盖印章或者签字的。

（三）项目负责人或者主要技术人员不是本单位人员的。

（四）投标保证金不是从投标供应商基本账户转出的。

（五）其他隐瞒真实情况、提供虚假资料的行为。

**二、本公司已充分知悉“与其他采购参加人串通投标”的法定情形，相关情形包括但不限于：**

（一）投标供应商之间相互约定给予未中标的供应商利益补偿。

（二）不同投标供应商的法定代表人、主要经营负责人、项目投标授权代表人、项目负责人、主要技术人员为同一人、属同一单位或者在同一单位缴纳社会保险。

（三）不同投标供应商的投标文件由同一单位或者同一人编制，或者由同一人分阶段参与编制的。

（四）不同投标供应商的投标文件或部分投标文件相互混装。

（五）不同投标供应商的投标文件内容存在非正常一致。

（六）由同一单位工作人员为两家以上（含两家）供应商进行同一项投标活动的。

（七）不同投标单位的投标报价呈规律性差异。

（八）不同投标单位的投标保证金从同一单位或者个人的账户转出。

（九）主管部门依照法律、法规认定的其他情形。

**三、本公司已充分知悉下列情形所对应的法律风险，并在投标前已对相关风险事项进行排查。**

（一）对于从其他主体获取的投标资料，供应商应审慎核查，确保投标资料的真实性。**如主管部门查实投标文件中存在虚假资料的，无论相关资料是否由第三方或本公司员工提供，均不影响主管部门对供应商存在“隐瞒真实情况，提供虚假资料”违法行为的认定。**

（二）对于涉及国家机关出具的公文、证件、证明材料等文件，一旦涉嫌虚假，经查实，主管部门将依法从严处理，并移送有关部门追究法律责任；涉嫌犯罪的，主管部门将一并移送司法机关追究法律责任。

（三）对于涉及安全生产、特种作业、抢险救灾、防疫等政府采购项目，供应商实施提供虚假资料、串通投标等违法行为的，主管部门将依法从严处理。

（四）供应商应严格规范项目授权代表、员工参与招标投标的行为，加强对投标文件的审核。项目授权代表、员工编制、递交投标文件等行为违反政府采购法律法规或招标文件要求的，投标供应商应当依法承担相应法律责任。

（五）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。相关情形如查实，依法作投标无效处理；涉嫌串通投标等违法行为的，主管部门将依法调查处理。

**四、本公司已充分知悉政府采购违法、违规行为的法律后果。**经查实，若投标供应商存在政府采购违法、违规行为，主管部门将依据《深圳经济特区政府采购条例》第五十七条的规定，处以一至三年内禁止参与本市政府采购，并由主管部门记入供应商诚信档案，处采购金额千分之十以上千分之二十以下罚款；情节严重的，取消参与本市政府采购资格，处采购金额千分之二十以上千分之三十以下罚款，并由市场监管部门依法吊销营业执照。

以下文字请投标供应商抄写并确认：“本公司已仔细阅读《政府采购违法行为风险知悉确认书》，充分知悉违法行为的法律后果，并承诺将严谨、诚信、依法依规参与政府采购活动”。

投标单位名称（单位盖公章）：

法定代表人或其委托代理人：

联系方式：

日期： 年 月 日

**附件5 报价单**

**报价单**

|  |  |
| --- | --- |
| 项目名称 |  |
| 投标人名称 |  |
| 法人代表 |  | 联系方式 |  |
| 项目联系人 |  | 联系方式 |  |
| 电子邮箱 |  |
| 联系地址 |  |
| 资质条件 | □符合正文中“供应商资格要求” □其他情况 （打“√”） |
| 投标报价(人民币) | 大写： 圆，小写： 元。 |
| 服务内容 |

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **服务频率** | **服务内容** |
| 1 | 渗透测试服务 | 1次/年 | 1.对单位4个重要信息系统〔即：（1）职业健康监督综合管理系统（包括：职业健康综合管理平台小程序）、（2）职业健康监护数据分析与监管系统、（3）民营医疗机构系统（包括：群众就医系统、民营医疗机构【门诊、诊所及医务室】服务系统、卫生监管系统）、（4）龙岗卫生监督在线培训系统〕进行渗透测试，包括信息系统收集、网络层渗透测试、应用层渗透测试、系统权限提升等各种黑客常用方法及手段，服务内容包括院内现有对外业务系统和后续新增的重要业务系统；2.协助对渗透测试过程中发现的问题进行整改；3.出具《渗透测试报告》。 |
| 2 | 业务逻辑漏洞专项检测 | 1次/年 | 1.对单位4个重要信息系统进行业务逻辑漏洞专项检测，对系统业务逻辑、数据流转各个环节进行检测，旨在发现系统功能技术实现上存在的逻辑问题，服务内容包括单位现有对外业务系统和后续新增的重要业务系统；2.协助单位对业务逻辑漏洞专项检测过程中发现的问题进行整改； 3.出具《业务逻辑漏洞专项检测报告》。 |
| 3 | 数据安全咨询、风险评估服务 | 1次/年 | 1.根据对单位的数据安全现状评估的结果，按照数据安全生命周期的规律，以开展数据共享开放业务的自身需求出发，规划设计适用于单位业务的数据安全保障体系，出具相应数据安全解决方案； 2.根据单位信息系统的实际情况开展安全风险进行识别与分析，采用传统的风险评估方法，从资产、威胁、脆弱性的角度，进行风险值量化。通过安全管理体系评估安全策略、规章制度、程序、表单体系的完整性，及制度是否得到贯彻执行，是否及时更新，是否全面覆盖需进行信息安全风险评估的信息系统。从风险管理的角度，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生时可能造成的危害程度，并提出有针对性的防护对策和整改措施，将风险控制在可接受的水平，最大程度地保障信息安全。 |
| 4 | 信息安全风险评估 | 1次/年 | 对单位进行全面性的风险评估，制定资产分析、威胁分析、弱点分析、现有措施分析、风险分析，给出针对性的风险处理方案、评估报告、评估总结，减少单位核心业务系统安全风险。 |
| 5 | 安全制度建设 | 1次/年 | 按照等级保护及相关主管部门、上级单位信息安全相关要求修订单位信息安全相关制度和规范。 |
| 6 | 网络安全应急响应 | 全年 | 根据单位实际情况，提供网络信息安全应急响应服务，包括：应急预案、事件处置及问题修复、报告输出；提供 7x24小时重大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。 |
| 7 | 安全意识培训 | 1次/年 | 1.对单位全员安全意识培训：从安全办公、个人信息安全、账户安全等方面普及安全常识，对常见的信息安全隐患进行分析、讲解，提高员工信息安全意识，告诉员工哪些网络行为不可为，如实施违法行为将承担法律责任，构成犯罪的须承担刑事责任，并开展《中华人民共和国网络安全法》《中华人民共和国密码法》《等级保护系列标准》《数据安全管理办法》等国家法律法规和标准培训；2.对网络安全管理相关部门进行安全管理工作方面培训。 |
| 8 | 漏洞扫描及加固服务 | 4次/年 | 1.对单位业务系统进行漏洞扫描；2.对单位业务系统相关服务器进行漏洞扫描；3.对单位业务系统和服务器漏洞加固指导；4.对单位业务系统和服务器漏洞加固后验证测试；5.对单位业务系统开展数据安全漏洞测试。 |
| 9 | 资产梳理 | 1次/年 | （一）信息资产梳理 1.统计所有在使用的计算机终端资产登记造册的完整性统计信息，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、计算机使用人身份证号码、计算机所属部门、计算机的物理位置等7个属性；2.信息系统资产包含：信息系统名称、定级情况、责任人及联系方式、访问URL(内网、公网)、系统架构（B/S或C/S）、系统相关主机IP清单、操作系统版本、托管物理位置、中间件类型和版本、数据库类型及版本、开发语言、开发框架等12个属性。（二）暴露面梳理1、通过主域名、IP网段、关键字、图标、备案号等方式主动发现单位所有互联网资产，资产包含子域名、IP、开放端口服务应用、资产变动情况、HTTP响应码、HTTP请求头、HTTP响应报文、端口banner、https证书信息、是否为登录入口、是否包含登录验证码等；2、根据单位提供的业务相关关键词或商标icon，搜索互联网上存活IP，识别出归属客户的互联网“影子资产”。 |
| 10 | 建立（修订）应急预案并开展应急演练 | 1次/年 | 根据《深圳市网络与信息安全突发事件应急预案》并结合单位实际情况制定与完善具有可操作性的网络及信息安全突发事件应急预案，确保应急预案可以适应信息系统的最新情况和外部的最新安全威胁。编写应急演练方案，定期开展安全事件应急演练，强化突发安全事件时单位的应急操作水平，最终实现应急人员、应急预案和应急操作的协调，提升单位的应急保障能力。 |
| 11 | 网络安全联合检查服务 | 全年按需 | 根据上级主管部门针对网络安全检查要求，提供安全迎检服务，以及现场检查迎检资料和技术支撑工作。 |
| 12 | 专项安全排查 | 全年按需 | 根据业界最新安全舆情、主管部门下发的漏洞和安全威胁开展安全排查并提供安全修复建议等。 |
| 13 | 驻点服务 | 2次/年 | 安排专业安全服务工程师进行驻场，专职提供技术服务，驻场工程师需具有一定的网络安全处理能力，能够实时监控网络情况，及时协助解决网络安全问题；具备日志分析能力能够更好地使用态势感知、防火墙、日志审计系统等安全设备，同时处理误报告警；同时沟通资源开展各项安全业务，协助办公室完成有关安全工作。  |
| 14 | 云防护 | 全年按需 | 1、提供云端防护账号交付，以 SaaS 的方式为用户提供网站安全防护服务（非硬件盒式WAF、非盒式抗DDoS攻击产品、非集成WAF及抗D功能的防火墙类产品，非虚拟机化WAF）；2、支持HTTPS网站防护。支持细粒度的WEB防护配置，至少支持对24大类Web安全漏洞类型对设置白名单，当设置生效后，针对某URL的该类WEB攻击不再防护（提供产品功能界面截图）；3、搜索引擎（百度、谷歌、必应、360、搜狗、神马搜索）及恶意爬虫防护，开启后即有默认防护配置（宽松/中等/严格），支持针对URL做单独的爬虫防护配置。支持配置强制缓存功能，当触发爬虫攻击防护时，可对用户自定义配置的URL按照选定的类型进行缓存，如延时、JS、图片、HTTPS验证。支持内置完备的敏感词信息库，可主动监测网站首页有无敏感词，支持URL匹配内容（提供产品功能界面截图）；4、支持WEB攻击统计报表，CC攻击统计报表，CC攻击URL TopN报表等。WEB攻击日志至少包含攻击类型、攻击IP、IP归属地、攻击URL及参数，攻击次数等参数。CC攻击日志至少包含攻击类型、攻击IP、IP归属地、攻击URL、攻击事件、攻击次数等参数（提供产品功能界面截图）；5、支持对Web攻击、CC攻击、爬虫攻击、DDOS攻击日志进行自定义攻击阈值告警。同时支持自定义统计周期、告警方式（邮件、短信）、告警接收人、告警接收组信息。支持将多个告警人添加为一个告警组，支持对同一告警组下所有告警人做相同告警配置（提供产品功能界面截图）；6、支持超级管理员、普通管理员、审计管理员等管理员角色。支持安卓/IOS版手机APP运维客户端，可支持手机接入防护、一键关站（一键处置）、一键回源、WEB防火墙开启/关闭、缓存开关设置、账号管理等功能（提供产品功能界面截图）；7、提供四份以上原厂商公开发布的专门针对中国的APT攻击事件研究报告。提供四份以上原厂商公开发布的专门针对网站安全相关安全研究报告（提供产品报告截图）。 |

 |
| 承诺书 | 本人承诺：1.本次报价材料真实有效，若因资料虚假造成损失，采购方有权依法追究本单位法律责任。2.完全满足本项目所需要提供服务的技术要求和商务要求。3.合作合同签署后由本单位组织开展该项工作，不随意更换工作人员，若需要更换技术人员，须提前告知采购方并征得采购方统一方可更换工作人员。投标供应商（盖章）：法人代表（授权代表）签字（盖章）：日期： |

附注：该表格双面打印，法人代表或授权代表在相应的栏目签字盖章。