## 第二章 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，按照招标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（WORD和PDF格式电子文档各1份）电子文档要求U盘，PDF格式有签字盖章，不留密码，无病毒，不压缩，密封提交，所有应答文件应于递交截止时间之前送达招标文件规定的地址。 |
| 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,作为招标代理服务费。低于人民币陆仟元的，按陆仟元计取。 |

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: 人民币贰拾捌万元（280,000.00），最高投标限价: 人民币贰拾捌万元（280,000.00）

（二）项目概况:

随着第一强制戒毒所业务不断实现信息化，各业务对信息系统的依赖越来越强。目前所里各类信息系统所依附运行的设备绝大多数已陈旧过保，硬件故障频发、维护工作量加大；在业务实现信息化的前提下，所内、外部用户对信息部门的服务也提出了非常高的要求；并且，在保证业务正常有效运行的同时，还需要切实做好信息安全保障工作和联络检查服务工作。但目前所内信息化办公室技术运维人员配置明显不足，无法很好地保证业务信息系统的正常运行及信息安全保障工作的有效落实，直接影响我所办公效率，影响工作的正常开展。

为切实做好信息安全保障工作、确保计算机类设施的正常运作、合理实现和支持业务自动化、及时解决问题故障、提高工作效率，使技术警力能够从繁琐的维护工作中解放出来，更好地为我所信息化建设事业作贡献。

### 四、项目技术要求

#### 1、整体服务要求

为切实做好信息安全保障工作、确保计算机类设施的正常运作、合理实现和支持业务自动化、及时解决问题故障、提高工作效率，使技术警力能够从繁琐的维护工作中解放出来，更好地为我所信息化建设事业作贡献。

**整体服务内容如下：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 说明 | 备注 |
| 1 | 电子政务运行维护 | 电脑终端、网络及中心机房维护；信息安全季度巡检；信息安全自查；信息安全专项工作（包括完善信息安全管理制度、安全防范措施落实、风险评估服务、定期网络安全扫瞄、定期对电脑终端进行扫描、应急服务、信息安全培训、终端安全检查）等。 |  |
| 2 | 专业技术人员服务 | 1、项目经理具有具有 ITIL Foundation 认证和工信部颁发的信息系统项目管理师认证；  2、技术人员具有 CISP工程师认证；  3、技术人员具有数通CCIE或HCIE认证证书。 4、具有项目管理、人员管理能力。  5、技术人员具有熟练使用新媒体平台（如抖音、微视频、微信等）进行视频制作、编辑和发布等能力。 |  |

#### 2、服务要求内容

**2.1电子政务运行维护服务**

电脑终端、网络及中心机房维护；信息安全季度巡检；信息安全自查；信息安全专项工作（包括完善信息安全管理制度、安全防范措施落实、风险评估服务、定期网络安全扫瞄、定期对电脑终端进行扫描、应急服务、信息安全培训、终端安全检查）等。

详细维护服务内容如下：

**2.1.1电脑终端、网络及中心机房维护工作内容**

一、PC桌面端

a)软件安装及配置

b)硬件及周外设备安装

c)硬件故障受理及对应

d)防病毒软件及补丁更新管理及确认

e)终端故障受理及处理

f)终端台帐管理及维护

g)常用办公软件使用方法培训及指导

二、网络设备维护

a)设备台帐管理及更新

b)网络设备日常维护（终端新增、线路调整等）

c)设备定期点检

d)设备故障受理及对应

e)网络局部变更对应及设置

f)设备更新及优化方案作成

三、服务器维护

a)服务器台帐管理及更新

b)服务器日常维护（补丁、防病毒软件等）

c)数据备份设置及备份结果确认

d)服务器系统安装及软件配置

e)服务器日常点检

f)服务器故障受理及对应

g)服务器更新及优化方案作成

四、网络中心机房精密空调维护

A.检查设备的运行状况

B.对需要进行清扫的机器进行除尘清扫

C.对设备内主要部件进行动态测试

D.检测机内易损单元 (空气过滤器、风机皮带和加湿罐)

E.检查设备的联接端子是否牢固

F.恢复设备运行, 检测设备的主要性能指标

G．对空调控制电路及设置参数检测

但是，维护保养服务不包括以下项目，如甲方需要下列服务，双方应另行协商约定收费标准：

G.设备以外的电源部分

H.安装场地的变动

I.设备或其他附件的搬运

J.不属于维修设备范围的和不是乙方所销售的其他附件或设备装置

K.由于事故、操作不当或忽视乙方书面要求等所造成的设备维修

L.由于与设备无关的事故（如破坏事故或其他原因）所造成的设备维修

M.设备的更新（如空调室内机和室外机等的整体更新）

**2.1.2 日常安全工作**

**2.1.2.1 季度安全巡检**

根据《2019年深圳市党政机关信息安全联合检查指南》的要求，需对服务器漏洞、设备漏洞、服务器安全策略、非涉密终端安全、非涉密终端保密清理、涉密终端安全状况进行检测，落实安全防护措施，保障业务系统的安全稳定运行。投标人每季度将发现的漏洞通报相关负责人进行加固，对已加固的漏洞进行复扫，确认整改效果。实施计划如下：

每季度第一个月中旬计划本季度扫描设备（含服务器、网络/安全设备和终端），与甲方确认巡检内容及时间。

每季度第二个月上旬开展设备安全检查（含漏洞扫描、安全策略核查、终端安全抽查），出具安全扫描报告并对发现的漏洞提出整改意见。

**2.1.2.2信息安全自查**

本年度信息安全自查工作包括：机房物理环境、网络管理、服务器管理、信息安全管理制度落实、维护管理及培训、场所录像管理工作、技术管理、保密管理等工作。工作安排如下：

每季度定时完成信息安全自查工作，收集《安全与保密实施方案》相关检查项原始信息。

每季度上旬分析信息安全制度，对需要改进的内容进行修订，交由信息安全领导小组进行审核并进行发布。在安全工作中落实制度和执行记录。

第季度在检查前审核自查总结报告，向深圳市司法局信息安全自查并总结报告。

**2.1.2.3 信息安全专项工作**

投标人根据《2019年深圳市党政机关信息安全联合检查指南》的要求，开展信息安全专项工作，投标人必需在每月28日前提交平台报告，报告的具体内容包括：

（1）完善信息安全管理制度

中标人完善深圳市司法局第一强制隔离戒毒所安全管理制度，建立适用于本单位的安全管理制度体系。

（2）安全防范措施落实

协助本单位运维人员对网络出口管理、网络安全审计、无线网络安全、涉密信息存储、终端资产登记、关键设备安全巡检、内外网防病毒等信息安全防范措施落实，并建立相关文档。

（3） 风险评估服务

需对深圳市司法局第一强制隔离戒毒所的各大信息管理系统、干警网络培训考核系统、强制隔离戒毒系统等进行的一次全面风险评估，分析系统所面临的各种风险，根据评估结果发现系统存在的安全问题，对严重的问题提出相应的风险控制策略。

（4）定期网络安全扫瞄

在网络中部署网络安全扫描系统，定期进行网络安全扫描。了解网络安全最新动向，及时获知漏洞补丁并更新其补丁

（5）定期对电脑终端进行扫描

每月定期对电脑终端涉密情况进行扫描，出具扫描截图报告，并协助深圳市司法局第一强制隔离戒毒所做好问题修复。

（6）应急服务

本项目要求提供365×24小时安全事件应急响应服务，当深圳市司法局第一强制隔离戒毒所安全评估范围内的系统发生安全事件时，立即（当日值班人员10分钟内，其他人员2小时内）到现场提供紧急响应服务，帮助深圳市司法局第一强制隔离戒毒所处理相关系统安全技术问题，保证系统的正常稳定运行。并根据市经贸信息委关于印发《深圳市网络与信息安全突发事件应急预案》的通知要求，8月上旬对应急预案进行修订，制定应急预案演练方案。8月中旬开展应急预案演练工作及整改总结。

（7）信息安全培训

根据《2019年深圳市党政机关信息安全联合检查指南》要求，投标人在9月中旬制定信息安全培训方案和计划；9月下旬开展信息安全意识培训。

（8）终端安全检查

终端安全检查包括非涉密终端内外网涉密信息、网络准入、内外网移动存储介质混插、防木马、防病毒系统、补丁升级系统、终端计算机密码强度、内网违规外联等内容和涉密终端安全状况的检查（涉密计算机不能接入党政内网、党政外网及互联网等任何网络、涉密计算机的操作系统补丁要及时更新、涉密计算机的防病毒软件要及时更新、涉密计算机不能使用普通移动存储介质、涉密机需要有专人管理）。该项工作在每季度安全巡检基础上进行的安全抽查。计划该项工作历时20个工作日，中标后1个月内开展该项工作。

**2.2专业技术人员服务**

投标人参与本项目的项目人员不少于5人，现场驻点服务人员不得少于2人，并在突发应急事件中能临时增加服务人员。

技术人员要求如下：

项目经理具有具有 ITIL Foundation 认证和工信部颁发的信息系统项目管理师认证；

技术人员具有 CISP工程师认证；

技术人员具有数通CCIE或HCIE认证证书。

技术人员具有项目管理、人员管理能力。

技术人员具有熟练使用新媒体平台（如抖音、微视频、微信等）进行视频制作、编辑和发布等能力。

所有复制的资料进行销毁，而且实行技术人员终身负责制，要求参与人员不得泄露任何建设情况。

#### 3、人员要求

投标人参与本项目的项目人员不少于5人，现场驻点服务人员不得少于2人，并在突发应急事件中能临时增加服务人员。

本项目的项目经理必须同时具有ITIL Foundation 认证和工信部颁发的信息系统项目管理师认证。

投标人必须为本项目成立本地化服务小组，由服务小组组长或主管统一负责，服务小组组长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，并具有CISP注册信息安全专业人员证书，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，服从甲方单位日常上班、值班制度，每天（含节假日）安排1人/24小时值班，落实甲方每天（含节假日）交接班制度。投标人派驻本项目的服务人员和服务小组组长必须固定，如有变更，必须经用户同意并签字确认。投标人必须提供人员管理及配备方案，并确保其人员的稳定性。

#### 4、运行维护配套服务工具要求

本次项目中标人需为维护服务提供专用配套设备服务，保障运维环境安全以及网络安全。该服务所配套设备须由中标人提供，服务到期后由中标人撤走。详细需求如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 详细技术要求 | 数量 | 单位 | 备注 |
| 1 | 配套设备设施服务 | 1.须提供交换机不少于2台，详细要求如下： | 1 | 项 |  |
| 1.1固定支持≥8个千兆电口，不少于2个千兆SFP口； |
| ▲1.2工作温度范围≥ -40℃ ~ 85 ℃，需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告扫描件，原件备查； |
| 1.3支持冗余输入，双路24VDC（12~36VDC），功耗<15W； |
| ▲1.4风暴抑制功能要求：产品需支持网络风暴抑制。需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告扫描件，原件备查； |
| ▲1.5适应性要求：产品应能在DC12V~DC36V范围内正常工作。需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告扫描件，原件备查； |
| ▲1.6稳定性要求：正常工作条件下，连续工作168h，不出现电、机械或操作系统的故障。需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告扫描件，原件备查； |
| ▲1.7 基于传输性能要求：因资源不足引起的丢包率，以端口能力100％发送数据，计算丢包率，丢包率应为0。需提供第三方检测机构出具的带有CMA和CNAS标识的检测报告扫描件，原件备查； |
| 1.8电源功耗＜30W、支持QoS、VLAN、IGMP Snooping等管理功能； |

#### 5、服务承诺要求

本项目涉及绩效评分情况，因此，投标人必需承诺严格按招标文件要求的来执行相对应的服务内容，本项目拟投入的技术成员资质情况，提供资质证书复印件，中标人需将驻点人员资质、专业、等级等证书复印件在履行合同期间交甲方单位统一保管，待合同期结束后返还，若合同履行期间必须更换人员时，将新派驻人员相关证书交至甲方后再将原驻点人员相关证书返还。

1、投标人承诺在本项目服务期间内，严格按照党政机关联合检查指南要求去完成，争取实现零扣分；

2、投标人承诺在本项目服务期间，驻场人员人数不得少于2人，确保桌面维护的质量与效果。

3、投标人公平竞争承诺：本公司保证所提交的相关资质文件和证明材料的真实性，有良好的历史诚信记录，并将依法参与本次项目投标的公平竞争，不得以任何不正当行为谋取不当利益，否则承担相应的法律责任。

#### 6、考核机制

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 维护项目 | 考核标准 | 扣分机制 | 惩罚机制 |
| 1 | PC桌面端 | 1.终端资产管理台帐（要求：全面，并实时更新）  2.终端维护记录（要求：实时记录）  3.终端维护及故障处理报告（要求：1次/季度）  4.终端安全（要求：安装指定的防病毒软件及开启有效的补丁系统升级策略） | 1）若发现执行记录和巡检计划未实施时，每1次扣1分  2）若发生故障时，未在要求时间内响应有并处理完成，每次扣1分。 | 总分60分：  1）每扣1分按合同金额1‰进行处罚。  2）每季度进行考核，考核结果双方达成一致后从合同余款中扣除。  3）扣除上限：不超过合同总额6%。 |
| 2 | 网络设备维护 | 1.网络设备管理台帐（要求：全面并实时更新）  2.网络设备日常维护记录（要求：实时记录）  3.网络设备定期巡检(要求：按巡检内容和计划执行)  4.设备维护及故障处理报告（要求：1次/季度）  5.设备更新及优化方案（要求：1 次/年） |
| 3 | 服务器维护 | 1.服务器管理台帐（要求：全面并实时更新）  2.服务器日常维护记录（要求：实时记录）  3.服务器定期巡检(要求：按巡检内容和计划执行)  4.服务器日常点检(要求：按巡检内容和计划执行)  服务器维护及故障处理报告（要求：1次/季度）  5.服务器更新更新及优化方案（要求：1 次/年） |
| 4 | 季度安全巡检 | 1.季度安全巡检报告（要求：1次/季度） | 1）若未按联合检查相关文件要求执行，造成年终联合检查扣分时，扣相应对等分值。 |
| 5 | 信息安全自查 | 2.信息安全自检报告（要求：1次/年） |
| 6 | 完善信息安全管理制度 | 1.信息安全管理制度确认及完善（要求：1次/年） |
| 7 | 安全防范措施落实 | 1.参照《深圳市党政机关2019年信息安全联合检查指南》、《2019年深圳市司法局信息安全与保密工作绩效实施方案》及《深圳市司法局直属各单位2019年信息安全与保密现场检查指标及评分标准》要求及时间进行实施；  （备注：参照当年度联合检查相关文件要求执行） |
| 8 | 风险评估服务 | 1.信息安全风险评估实施（要求：1次/年） |
| 9 | 定期网络安全扫瞄 | 1.季度安全巡检报告（要求：1次/季度） |
| 10 | 定期对电脑终端进行扫描 | 1.月度安全巡检报告（要求：1次/月） |
| 11 | 人员管理 | 1.按甲方出勤管理规定执行 | 1）若发现不遵守甲方出勤要求，每2次扣1分 |
| 12 | 信息安全意识培训 | 按照经信委规定的年度培训次数进行：  全员安全意识培训（要求：1次/年） | 1）未完成扣5分 |

#### 7、资料保密

所有投标人均需对招标文件及所含附件内容保密，未在招标人授权范围内不得向本单位以外任何单位及个人泄露本包招标内容及文件，否则依据国家相关法律法规要求追究泄露单位及个人的法律责任。投标人必须在中标后与招标人签订保密协议，承诺不将任何涉及本项目的信息向外界泄露。

### 五、项目商务要求

（一）服务期限：合同签订之日起12个月。该项目为长期服务项目，根据供应商的履约情况，合同期限可以延续，但最长不得超过三十六个月。

（二）服务地点：深圳市司法局第一强制隔离戒毒所

（三）付款方式：

1、合同签订后 1 个月内，甲方向乙方支付合同总价40%的款项。

2、合同签订后 6个月内，甲方向乙方支付合同总价30 %的款项。

3、合同结束后 1 个月内，甲方向乙方支付合同总价30%的款项。

（四）质量考核验收标准及违约金

1.质量考核验收标准：

1）服务经过双方检验认可后，签署验收报告。

2）当满足以下条件时，采购人才向中标人签发验收报告：

a、中标人已按照合同规定提供了全部技术资料。

b、服务项目符合招标文件的服务要求。

2.违约金：以合同签订为准

### 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。