招 标 文 件

（服务类）

采购项目名称：温江区电子政务外网安全支撑运维服务(二次)

采购项目编号：**N5101152024000008**

成都市温江区智慧蓉城运行中心

成都鑫源至成工程项目管理咨询有限公司共同编制

2024年**03**月**06**日

第一章 投标邀请

成都鑫源至成工程项目管理咨询有限公司（以下简称“代理机构”）受成都市温江区智慧蓉城运行中心委托，拟对温江区电子政务外网安全支撑运维服务(二次)进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：N5101152024000008

二、采购项目名称：温江区电子政务外网安全支撑运维服务(二次)

三、招标项目简介

电子政务外网是我国政府信息化建设的关键，随着政府部门信息化程度的提高，对信息系统的依赖程度越来越高。同时，整个电子政务外网的信息系统所面临的各种安全风险也日益严重，如何更好地为电子政务外网和电子政务信息系统提供安全保障，确保电子政务外网的安全运行和信息化的健康发展是成都市电子政务网络和信息系统建设所面临的一个主要问题。 为了提高温江区电子政务外网应对网络安全事件的能力，扎实有效加强信息安全防护能力，预防和减少网络安全事件造成的损失和危害，为温江区电子政务外网的网络及各类信息系统的安全、可靠、稳定、高效的运行提供良好的基础和强有力的保障，拟通过本次服务项目，对温江区电子政务外网网络安全事件进行安全监测、分析、阻断、处置，全面提升整体网络安全风险监管及防御能力，支撑各类大型网络安全保障工作，有效挖掘网络安全设备日志，充分应对来自外部的威胁，保障不出网络安全事故，进一步加强温江区电子政务外网的安全防护。

四、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

执行政府采购促进中小企业发展的相关政策：

采购包1（合同包一）：属于专门面向小微企业采购。

注：监狱企业和残疾人福利性单位视同小微企业，符合中小企业划分标准的个体工商户视同中小企业。

（三）本项目的特定资格要求：

采购包1：

无

五、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：四川省政府采购一体化平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过四川政府采购网（www.ccgp-sichuan.gov.cn）首页供应商用户登录四川省政府采购一体化平台（以下简称“采购一体化平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在四川政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用采购一体化平台前，应当按照要求完成供应商注册和信息完善，加入采购一体化平台供应商库。

(二)供应商应当使用纳入全国公共资源交易平台（四川省）数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录采购一体化平台进行的一切操作和资料传递，以及加盖电子签章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身

份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看四川政府采购网-办事指南。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）采购一体化平台技术支持：

在线客服：通过四川政府采购网-在线客服进行咨询

400服务电话：4001600900

CA及签章服务：通过四川政府采购网-办事指南进行查询

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告或邀请书

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标文件上传至项目电子化交易系统，免费向供应商提供。供应商通过项目电子化交易系统获取招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的招标文件，供应商应当重新获取招标文件。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

注：获取的招标文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告或邀请书

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在四川政府采购网以公告形式发布

九、供应商信用融资

根据《四川省财政厅关于推进四川省政府采购供应商信用融资工作的通知》（川财采〔2018〕123号）文件，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录四川政府采购网—金融服务平台，选择符合自身情况的“政采贷”银行及其产品，凭项目成交结果、成交通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

十、联系方式

采购人： 成都市温江区智慧蓉城运行中心

地址： 温江区人和路733号

邮编： 611130

联系人： 杨成庆

联系电话： 82721133

代理机构：成都鑫源至成工程项目管理咨询有限公司

地址： 成都市武侯区一环路南一段20号普利大厦B座307室

邮编： 610000

联系人： 余先生

联系电话： 028-86610889/15882084014

第二章 投标人须知

2.1投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	本项目各包采购预算金额如下： 采购包1：1,490,000.00元 投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。
2	最高限价（实质性要求）	详见第三章。 投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。
3	评标方法	采购包1：综合评分法 （详见第五章）
4	是否接受联合体	采购包1：不接受联合体
5	落实节能、环保、无线局域网	1.根据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。 2.本项目采购 无 产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。 3.本项目采购 无 产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购 无 产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/响应报价相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。 4.响应产品属于中国政府采购网公布的《无线局域网认证产品政府采购清单》且在有效期内的，按《财政部国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号）要求优先采购。
6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第五章。

7	充分、公平竞争保障措施（实质性要求）	核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。 使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。 采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。 核心产品清单详见第三章。 在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
9	投标保证金	本项目不收取投标保证金。
10	履约保证金（实质性要求）	采购包1：不收取
11	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。
12	招标代理服务费（实质性要求）	本项目收取代理服务费 代理服务费用收取对象：中标/成交供应商 代理服务费收费标准：采购代理机构按照成本加合理利润原则，向中标人收取招标代理服务费。
13	采购结果公告	采购结果将在四川政府采购网予以公告。
14	中标通知书	采购结果公告后，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
15	政府采购合同公告、备案	政府采购合同签订之日起2个工作日内，采购人将政府采购合同在四川政府采购网予以公告；政府采购合同签订之日起7个工作日内，采购人将政府采购合同报本级财政部门备案。
16	进口产品	不允许（实质性要求）
17	是否组织潜在投标人现场考察	采购包1：否

18	特殊情况	出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。
19	报价/分值精确度	所有数据项默认最多可输入/展示至小数点后2位，超出小数点位的数值采用四舍五入的方式进行精确。

2.2总则

2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由成都市温江区智慧蓉城运行中心和成都鑫源至成工程项目管理咨询有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由成都市温江区智慧蓉城运行中心负责解释。除上述招标文件内容，其他内容由成都鑫源至成工程项目管理咨询有限公司负责解释。

2.2.2有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次招标的采购人是成都市温江区智慧蓉城运行中心。

二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物及相应服务的法人、其他组织或者自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是成都鑫源至成工程项目管理咨询有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成评标委员会组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选供应商等活动。

2.3招标文件

2.3.1招标文件的构成

一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：

（一）投标邀请；

（二）投标人须知；

（三）招标项目技术、服务、商务及其他要求；

（四）资格审查；

（五）评标办法；

（六）投标文件格式；

（七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面作出实质性

响应所产生的风险由投标人承担。

2.3.2招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在四川政府采购网发布更正公告，投标人应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响投标文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4投标文件

2.4.1投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，评标委员会将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对投标人的不利后果，由投标人承担。

2.4.2计量单位（实质性要求）

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3投标货币（实质性要求）

本次项目均以人民币报价。

2.4.4知识产权（实质性要求）

一、投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、投标人将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，投标人需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5投标文件的组成

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

2.4.6投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子印章，投标人未在规定时间内确认的，其投标无效。

2.4.8投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9投标文件的制作、签章和加密（实质性要求）

一、投标文件应当根据招标文件进行编制，投标人应通过四川政府采购网-办事指南下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5开标、资格审查、评标和中标

2.5.1开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或成功提交和解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

投标文件开启时间前，供应商登录项目电子化交易系统-“开标/开启大厅”，等待代理机构开标。

投标文件提交截止时间前30分钟，投标人登录项目电子化交易系统-“开标/开启大厅”参与开标。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

2.5.2查询及使用信用记录

开标结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、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中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，将对所有联合体

成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3资格审查

详见招标文件第四章。

2.5.4评标

详见招标文件第五章。

2.5.5中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在四川政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标供应商均具有法律效力。

2.6签订及履行合同和验收

2.6.1签订合同

一、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包；

2.6.2.2合同转包

一、严禁中标供应商将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、中标供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，在不改变合同其他条款的前提下，可以与中标人协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2.6.4履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

2.6.5履约验收方案

采购包1：

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：分段/分期验收

7）履约验收时间：

供应商提出验收申请之日起7日内组织验收

8）验收组织的其他事项：无

9）技术履约验收内容：服务提供商应针对本项目建立完善的质量管理体系，并配备相应的人员或机构，确保项目服务质量的落实和保证。 服务提供商应配合采购人按照采购人制定的服务考核指标定期对本项目各项服务进行质量考核。 服务质量主要指标。要求保证设备可用性不低于99.95%，年度服务费用结算将结合服务质量考核结果，按比例扣除相应服务费用。 应用系统可用性=（365×24×60×60秒－单个应用失效时间之和（秒））/（365×24×60×60秒）；即：全年失效时间不超过365×24×60×0.0005=262.8分钟。应用失效时间指服务提供商提供的安全服务等方面出现的严重问题引起应用系统失效时间。经采购人认定由非供应商引起的系统失效（如不可抗力）不包含在内。 采购人有权对服务提供商的驻场人员的出勤率及技术水平进行考评，如果达不到要求，有权要求服务提供商更换驻场人员，直到采购人满意为止。 本项目中所有服务以签署验收报告作为验收标志，同时作为支付尾款的条件。

10）商务履约验收内容：服务提供商应针对本项目建立完善的质量管理体系，并配备相应的人员或机构，确保项目服务质量的落实和保证。 服务提供商应配合采购人按照采购人制定的服务考核指标定期对本项目各项服务进行质量考核。 服务质量主要指标。要求保证设备可用性不低于99.95%，年度服务费用结算将结合服务质量考核结果，按比例扣除相应服务费用。 应用系统可用性=（365×24×60×60秒－单个应用失效时间之和（秒））/（365×24×60×60秒）；即：全年失效时间不超过365×24×60×0.0005=262.8分钟。应用失效时间指服务提供商提供的安全服务等方面出现的严重问题引起应用系统失效时间。经采购人认定由非供应商引起的系统失效（如不可抗力）不包含在内。 采购人有权对服务提供商的驻场人员的出勤率及技术水平进行考评，如果达不到要求，有权要求服务提供商更换驻场人员，直到采购人满意为止。 本项目中所有服务以签署验收报告作为验收标志，同时作为支付尾款的条件。

11）履约验收标准：

服务提供商应针对本项目建立完善的质量管理体系，并配备相应的人员或机构，确保项目服务质量的落实和保证。服务提供商应配合采购人按照采购人制定的服务考核指标定期对本项目各项服务进行质量考核。 服务质量主要指标。要求保证设备可用性不低于99.95%，年度服务费用结算将结合服务质量考核结果，按比例扣除相应服务费用。 应用系统可用性=（365×24×60×60秒－单个应用失效时间之和（秒））/（365×24×60×60秒）；即：全年失效时间不超过365×24×60×0.0005=262.8分钟。应用失效时间指服务提供商提供的安全服务等方面出现的严重问题引起应用系统失效时间。经采购人认定由非供应商引起的系统失效（如不可抗力）不包含在内。 采购人有权对服务提供商的驻场人员的出勤率及技术水平进行考评，如果达不到要求，有权要求服务提供商更换驻场人员，直到采购人满意为止。 本项目中所有服务以签署验收报告作为验收标志，同时作为支付尾款的条件。

12）履约验收其他事项：无

2.6.6资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7纪律要求

2.7.1评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响评标过程和结果。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2投标人不得具有的情形（实质性要求）

投标人参加投标不得有下列情形：

一、有下列情形之一的，视为投标人串通投标：

（一）不同投标人的投标文件由同一单位或者个人编制；

（二）不同投标人委托同一单位或者个人办理投标事宜；

（三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（五）不同投标人的投标文件相互混装；

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照招标文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

投标人有上述情形的，按照规定追究法律责任，具有前述一至十三条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

2.7.3采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与投标人有下列利害关系之一的，应当回避：

（1）参加采购活动前3年内与投标人存在劳动关系；

（2）参加采购活动前3年内担任投标人的董事、监事；

（3）参加采购活动前3年内是投标人的控股股东或者实际控制人；

（4）与投标人的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（5）与投标人有其他可能影响政府采购活动公平、公正进行的关系。

投标人认为采购人员及相关人员与其他投标人有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

2.8询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对招标文件中采购需求的询问、质疑由 成都鑫源至成工程项目管理咨询有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由成都鑫源至成工程项目管理咨询有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 成都鑫源至成工程项目管理咨询有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处

理解决（包含但不限于文字错误、标点符号、不影响投标文件的编制的情形）。

四、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（二）对采购过程提出质疑的，为各采购程序环节结束之日；

（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料

（一）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）

（二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；

（三）法定代表人或主要负责人身份证复印件1份；

（四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；

（五）针对质疑事项必要的证明材料（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：余先生

联系电话：028-82668681/15882084014

地址：成都市武侯区一环路南一段20号普利大厦B座307室

邮编：610000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出招标文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1采购项目概况

1.项目实施的必要性与可行性：在温江区电子政务外网网络中心机房，统一托管了全区各部门行业应用和网站服务器，服务器数量350台左右。同时在云计算中心也通过服务器虚拟化部署了多部门的业务系统。在其运行业务系统的包括组织、人事、财政、国资、卫生、教育、规划、政务中心等重要信息系统和网站，基本涵盖了温江区各类应用系统基本信息、政府资产信息、各级政府工作人员信息、经济运行数据、各类项目信息等各个领域信息数据，信息数据量相对比较庞大。前期，温江区电子政务外网已对互联网出口、服务器区域、云计算中心区域等重要区域进行了安全域的划分和隔离防护。内部安全态势进行了大数据分析对网络安全态势进行感知和风险应对。随着智慧蓉城建设的不断深入，构建立体化网络安全态势感知、监测预警和事件相应处置能力的要求持续加强。 2.项目实施内容： 构建持续的常态化安全运维保障服务： 电子政务外网是我国政府信息化建设的关键，随着政府部门信息化程度的提高，对信息系统的依赖程度越来越高。同时，整个电子政务外网的信息系统所面临的各种安全风险也日益严重，如何更好地为电子政务外网和电子政务信息系统提供安全保障，确保电子政务外网的安全运行和信息化的健康发展是成都市电子政务网络和信息系统建设所面临的一个主要问题。 为了提高温江区电子政务外网应对网络安全事件的能力，扎实有效加强信息安全防护能力，预防和减少网络安全事件造成的损失和危害，为温江区电子政务外网的网络及各类信息系统的安全、可靠、稳定、高效的运行提供良好的基础和强有力的保障，拟通过本次服务项目，对温江区电子政务外网网络安全事件进行安全监测、分析、阻断、处置，全面提升整体网络安全风险监管及防御能力，支撑各类大型网络安全保障工作，有效挖掘网络安全设备日志，充分应对来自外部的威胁，保障不出网络安全事故，进一步加强温江区电子政务外网的安全防护。

3.2服务内容及服务要求

3.2.1服务内容

采购包1：

采购包预算金额（元）: 1,490,000.00

采购包最高限价（元）: 1,490,000.00

序号	标的名称	数量	标的金额 （元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	安全运维服务	1.00	1,490,000.00	包	信息传输业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：安全运维服务

参数性质	序号	技术参数与性能指标

一、安全服务方案

1.安全运维保障服务总体思路

为应对当前温江区电子政务外网可能存在的病毒、木马、系统漏洞等风险，实现风险识别与风险闭环，保障业务系统安全运转，需要做到“持续有效”，两者缺一不可，若安全机制非持续保障的，则说明面对外界威胁的持续变化无法持续保障业务安全；若安全机制非有效的，则说明当前安全机制存在短板。那么，网络安全持续有效至少应该具备以下三个能力:

持续降低资产病毒、木马、系统漏洞等风险，减少被黑客利用的机会；

持续保持安全策略有效性，精准抵御高级威胁；

持续监测安全事件，第一时间遏制，降低损失。

因此，针对目前温江区电子政务外网的安全现状和存在问题，本次安全服务项目提出以下解决方案：

构建持续的常态化安全运维保障服务：

（1）通过定期的漏洞扫描、恶意软件扫描、风险评估、渗透测试等安全风险识别手段，对网络中存在的安全风险提前全面识别；

（2）通过7*24h对网络中的异常流量、安全日志进行全面系统的分析，及时发现网络中发生的安全威胁、事件，进行持续监测、快速响应闭环；

（3）通过对安全事件的告警及威胁进行持续监测，做到政务外网病毒、木马、系统漏洞等提前发现，持续保障网络安全有效

（4）通过常态化本地安全驻场服务，构建及时动态的闭环体系。

2.常态安全运维保障服务

2.1.本地驻场安全运维服务

2.1.1服务目标

本地驻场安全运维服务提供现有及服务期内新增的各安全系统的监测服务，服务期内服务提供商安排工程师常驻用户现场定期对现有的安全设备的日志进行分析，对存在问题进行及时处理，进一步降低网络中安全威胁，定期对信息网络系统进行安全健康检查，协助温江区电子政务外网用户完成有关信息安全应急响应工作，提供安全预警服务，定期发送安全事件通告和高危安全事件的紧急通告，对发现的安全事件提出整改方案和整改计划，并牵头进行整改实施工作。

2.1.2服务内容

（1）温江区电子政务外网里的资产进行梳定期梳理

（2）温江区电子政务外网里包括交换机、防火墙、入侵防御、漏洞扫描、安全大数据平台等安全设备的部署和维护以及服务器、虚拟机、云平台涉及安全问题的管理维护工作。

（3）负责对机房内在用的网络安全设备进行日常设备维护，同时对安全设备的防护代码及补丁进行升级、策略进行调整，通过对安全设备的合理利用和部署，减少网络病毒、木马、黑客等网络不良因毒对网络的影响，保护网络及业务系统和数据。

（4）对用户的相关系统的新建、扩容、升级等计划提供专业的技术建议、设计服务和技术指导，协助用户完成相关技术方案的制定和辅助用户完成相关技术方案的实施。

（5）维护期内增加的网络安全设备。

（6）建立突发事故处理的服务流程，对于安全系统出现的故障，迅速做出反应及时处理，以保障安全系统的正常运行。

（7）设备资料归档：对维护的网络安全设备的基本情况建档，并随时跟踪更新。建档的原则是以单台设备为单位建立。档案资料包括网络拓扑、硬件配置清单及版本、软件系统版本及功能、当前使用状况、网管参数、当前主要配置参数记录等。

定期巡检：为尽早发现各种隐患，定期对机房安全设备和主机进行巡检。

2.1.3服务方法

服务方式包括：7×24小时热线支持、7×8小时常驻现场服务、7×24小时远程服务、二线支持现场服务等。现场驻场至少1人。

2.1.3.1资产管理

每季度进行资产梳理。

（1）在资产梳理与管理中，主要识别内网及电子政务外网侧的如下类型资产：

服务器类资产：服务器类资产发现与梳理工作，备案确认的资产，备案信息包括IP、所属系统、操作系统类型、中间件、数据库、用途、所属业务单位、运维责任人、联系方式。与各个单位相关人员对未知资产进行确认。

网络设备类资产：网络设备类资产发现与梳理工作，备案确认的资产，备案信息包括IP、所属系统、设备类型、管理方式、用途、所属业务单位、运维责任人、联系方式。与各个单位对未知资产进行确认。

安全设备资产：安全设备资产发现与梳理工作，备案确认的资产，备案信息包括IP、所属系统、设备类型、管理方式、用途、所属业务单位、运维责任人、联系方式。与各个单位相关人员对未知资产进行确认。

互联网业务资产：互联网业务资产发现与梳理工作，备案确认的资产，备案信息包括域名、数据库、中间件、管理方式、用途、所属业务单位、运维责任人、联系方式。

内网业务资产：内网业务资产发现与梳理工作，备案确认的资产，备案信息包括域名、数据库、中间件、管理方式、用途、所属业务单位、运维责任人、联系方式。

影子资产：影子资产，属于一种不透明的资产，比如部门个人搭建的服务器或历史遗留无责任归属的资产等等。

（2）应重点关注服务关键内容资产：

梳理资产：需要识别保护对象，以互联网侧的资产为主，梳理包含业务系统、服务器、安全设备、关键网络设备等，其中脱离IT管理、控制及安全审计的影子资产的挖掘是重中之重，以此明确互联网暴露面。

自查自检：针对保护对象开展自查自检工作，通过漏洞扫描、基线核查、红队检测、攻击路径分析、失陷检测等方式检视现存的安全缺陷，以明确后期加固建设工作的方向及重点。

2.1.3.2定期安全巡检

每周定期进行安全巡检，包括安全设备巡检、策略巡检和安全事件分析总结等。

安全巡检服务主要对生产环境以及环境内的防火墙、路由器、交换机、服务器、云管理平台、虚拟机等设备进行定期安全巡检工作，发现是否存在安全隐患和可疑事件，运行是否正常。巡检内容包括但不限于设备的运行状态、策略、配置、日志分析等。

1、日志获取：巡检人员在现场获取业务支持系统中的安全设备、监控工具等的相关信息，并统一存储在安全信息库中。

2、事件确认：监控工具或安全设备报告的事件中有些是误报有些是有威胁的攻击，需要考虑网络环境、安全防护措施、操作系统、系统补丁、应用情况等情况。这样经过巡检人员及时分析确认的事件才有实际意义，可以用来触发事件响应，包括应急支持等。

3、专家分析：信息安全专家对数据挖掘专家的日志做进一步的分析，从中发现可疑的行为和事件，并判断这种行为对系统可能造成的影响以及影响的程度；分析可疑的节点行为，评估其对整个业务支持系统造成的影响，并建立特殊的黑名单机制，对其做进一步的监控；对需要响应的疑点、病毒事件或安全事件及时通告给的紧急事件响应小组。

安全巡检报告是为温江区电子政务外网深刻了解自身业务支持系统安全状况的一种有效形式，它主要涉及了如下的内容：

1、主体事件统计：明确了在温江区电子政务外网业务支持系统中的主要事件，有助于温江区电子政务外网了解其网络资源的利用效能。

2、病毒与安全危险：记录了业务支持系统中曾经出现过的病毒或者安全危险，记录了病毒或者安全事件的来源与目标，病毒感染范围、削除时限。有助于温江区电子政务外网了解在其业务支持系统中各个终端的病毒感染、安全事件状况以及存在的内部与外部的安全隐患。

3、特殊事件分析：对于可疑安全事件进行深层次的分析，判断其可能造成的伤害和影响，并提供对这些事件的处理建议。

4、系统安全建议：根据分析的结果，对业务支持系统设备提出包括零入侵攻击保障时段时长频度，重点保护日期、时段及要求在内的合理化建议。

2.1.3.3定期安全检查

每季度对服务器、网络设备、数据库、应用系统等进行一次全面的系统漏洞扫描和安全配置检查，清晰定性安全风险，给出修复建议和预防措施，并进行跟踪处理；每季度对的外网网站进行渗透测试服务，挖掘应用风险漏洞，避免网站被篡改和控制。

漏洞扫描

安全扫描是指为温江区电子政务外网提供安全扫描产品/工具对温江区电子政务外网授权的信息系统进行脆弱性评估，获得设备---漏洞对应及分布情况，并提供可操作的安全建议或临时解决办法。

安全扫描主要包括如下几个方面：

服务器主机系统安全漏洞检查（工具扫描）；

数据库系统安全漏洞检查（工具扫描）；

中间件安全漏洞检查（工具扫描）；

网络设备漏洞检查（工具扫描）；

安全设备漏洞检查（工具扫描）；

系统开放端口检查

系统端口扫描是通过连接到目标系统的TCP协议或UDP协议端口，来确定什么服务正在运行。一般扫描端口有如下的目的：

判断目标主机上开放了哪些服务

判断目标主机的操作系统类型

通过实施端口扫描掌握了目标主机开放了哪些服务，运行何种操作系统，根据端口扫描结果，结合业务特点，提出关闭相关非必要服务的建议。

弱密码检查

弱密码检查是指使用安全扫描产品/工具对附件温江区电子政务外网授权的信息系统进行弱口令扫描，获得设备---弱口令对应及分布情况，并提供可操作的安全建议或临时解决办法。

弱密码扫描主要包括如下几个方面：

服务器主机系统弱口令检查（工具扫描）；

数据库系统弱口令检查（工具扫描）；

中间件弱口令检查（工具扫描）；

网络设备弱口令检查（工具扫描）；

安全设备弱口令检查（工具扫描）；

主机常规后门检查

检查目标主机、网站的系统后门、WEBSHELL、异常帐号、日志量等。对于出现的后门和WEBSHELL等问题给出清除建议和补救措施。

主机常规后门检查列表

检查项目	说明	检查方式/工具
账号异常	检查系统账号/应用账号是否异常	手工
系统后门	检查系统是否被植入后门	Windows:PowerTool、XueTr等 Linux:RootkitHunter、chkrootkit
系统补丁	检查系统补丁安装情况	手工
软件版本	检查所安装软件的该版本是否存在漏洞	手工
系统日志	检查系统日志有无异常	手工
Web日志	检查web日志，分析有无被攻击迹象	手工/loganalysis等
Webshell	检查网站是否被植入webshell	手工/D盾_Web查杀等

安全修复复查

在全面检查完成后，将根据检查结果提供检查报告，并在检查报告中提出加固建议。加固完成后，将次进行相关安全问题复查，直到全部问题得到修复。

2.1.3.4安全通告与预警

在多年的安全服务经验的积累上，将根据客户的安全预警需求，组织安全信息定期通告，及时告知客户最新的安全事件（0day系统漏洞、网络攻击）的解决办法。对于重大高危安全问题将及时通报。

1、将向客户提供最新发现的各种操作系统、数据库、网络设备、应用软件的安全漏洞信息和病毒信息，以满足安全预警服务的基本需要。此项服务由基础研究部进行追踪，最终根据预警级别，通过邮件等方式提供给客户指定接口人。

2、基础研究部承诺为客户提供包括漏洞的名称、级别、受影响的软件、检测方法、应急措施和根除措施等内容的安全预警信息。

3、提供的安全预警信息将以电子邮件的方式发送到客户指定的邮箱中。一旦基础研究部预警小组确认安全漏洞，这个发送过程将由安全预警平台的邮件系统自动发送。

4、对于安全研究小组认定的严重、紧急的安全预警信息，将以电话、短信、传真的方式通知客户的预警工作接口人。并确保严重漏洞得到客户预警接口人的接受确认。

5、向客户提供的安全预警信息将先于对外公布至少1天时间。对有些未发现有效的最终解决方案的安全漏洞，将为客户提供临时解决方案，并至少推迟1周时间后再向外公布此安全漏洞。

6、针对为客户提供的安全预警信息的相关内容，由的安全专家向客户提供7*24小时的专人电话支持服务。

2.1.3.5应急响应服务

目前许多温江区电子政务外网自身尚没有足够的资源和能力对安全事故做出反应，甚至在当今的信息社会，更多的组织还没有准备面对信息安全问题的挑战。网络安全的发展日新月异，谁也无法实现一劳永逸的安全服务，所以当紧急安全问题发生，一般技术人员又无法迅速解决的时候，及时发现问题、解决问题就必须依靠紧急响应来实现。

应急响应的作用主要表现在事先的充分准备和事件发生后采取的措施两个方面的作用。

一方面是事先的充分准备。这方面在管理上包括安全培训、制订安全政策和应急预案以及风险分析等，技术上则要增加系统安全性，如备份、打补丁了，升级系统与软件，有条件的可以安装防火墙，入侵检测工具（IDS）和杀毒工具等。

另一方面事件发生后的采取的抑制、根除和恢复等措施。其目的在于尽可能的减少损失或尽快恢复正常运行。如收集系统特征，检测病毒、后门等恶意代码，隔离、限制或关闭网络服务，系统恢复，反击，跟踪总结等活动。

以上两个方面的工作是相互补充的。首先，事前的计划和准备为事件发生后的响应动作提供了指导框架，否则，响应动作将陷入混乱，而这些毫无章法的响应动作有可能造成比事件本身更大的损失。其次，事后的响应可能发

现事前计划的不足，吸取教训。从而进一步完善安全计划。因此，这两个方面应该形成一种正反馈的机制，逐步强化组织的安全防范体系。

2.1.4服务成果

本次安全驻场运维服务所提交的交付物包括但不限于以下成果：

《XXX驻场服务手册》

《安全值守月度工作计划》

《安全值守月度报告》

《安全值守周报》

《XX资产梳理报告》

《XX安全策略优化报告》

《XX季度漏洞扫描报告》

《重保值守报告》

《安全加固方案》

《安全加固报告》

《安全运营月报》

《变更申请表》

《变更执行记录表》

《系统与设备测试记录》

《系统问题跟踪与记录单》

《检查总结报告》

2.2安全风险评估服务

2.2.1服务内容

通过安全风险评估服务，定期识别政务外网资产中存在的病毒、木马、系统漏洞等潜在安全风险，输出安全风险清单并及时进行修复。风险评估的服务内容包含如下几个环节：

2.2.1.1资产识别

资产是风险评估的最终评估对象，风险的所有重要因素都紧紧围绕着资产，而威胁性和脆弱性都是针对资产客观存在的。因此风险评估的第一步是确定信息系统的资产，并明确资产的价值，资产的价值是由用户在业务战略的实现过程中对资产的依赖性以及安全事件发生后对组织、供应商、合作伙伴、用户和其他利益相关方的影响程度来衡量的。资产的范围很广，对组织具有价值的信息或资源都是信息资产，使用自研漏扫工具对包括：业务系统、服务器、安全设备、网络设备等进行自动化扫描发现、识别、评估。资产的识别和评估应当从关键业务开始，最终覆盖所有的资产，之后根据业务对资产的实际依赖程度进行区分是否为重要资产，脆弱性识别、威胁识别、风险分析等后期工作将只针对于重要资产进行识别。

资产识别主要使用工具扫描探测、人工访谈调研与文档审阅等方式进行收集资产。开展深入的信息资产识别时，主要收集以下几个方面的资产：业务应用（信息系统）、文档和数据(网络拓扑图、信息系统相关文档、信息系统数据库数据)、软硬件资产（服务器设备、安全设备、存储设备、系统软件、应用软件等）、物理环境（机房等）、组织管理（规章制度等）、人力资源资产（组织架构、岗位职责等）。

2.2.1.2脆弱性评估

脆弱性是指资产中能被威胁所利用的弱点，它存在于物理环境、硬件、软件、业务系统等各个方面，这些都可能被各种安全威胁利用来侵害用户的资产，让资产的价值受损。各种脆弱性自身并不会造成什么危害，只有在被各种安全威胁利用后才可能造成相应的危害。评估弱点时需要考虑两个因素，一个是弱点被威胁利用后产生影响或危害的严重程度，另一个是弱点的暴露程度，即被利用的容易程度。需要注意的是，弱点是威胁发生的直接条件，如

果资产没有弱点或者弱点很轻微，威胁源就很难利用其损害资产，哪怕它的能力多高、动机多么强烈。因此评判脆弱性的级别不仅需要考虑被利用的破坏力，还需要考虑被利用的几率，经此分析出的弱点才更符合用户的实际情况。主要工作如下：

漏洞扫描：使用漏洞扫描功能的自研工具，能够快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全漏洞，并给出关于安全隐患的详细信息。

基线配置核查：使用基线配置核查功能的自研工具，安全基线是一个信息系统的最小安全保证，即该信息系统最基本需要满足的安全配置要求。基线核查是信息系统及所属设备等在特定时期内，根据自身需求、部署环境和承载业务要求应满足的基本安全配置，全面集中检查和分析各类系统存在的本地安全配置问题。

人工审核：通过人工的资料审阅、现场勘查、上机测试等方法，人为的对相关资料进行筛选核实与审查，从而大幅度降低工具的误判率，并能发现一些自动化工具无法发现的一些管理层面、逻辑层面、工作流程层面的安全隐患。

调研访谈：调研访谈是针对特定环境下进行的一种信息安全内容的收集方式，针对用户现有的安全状态调研和安全措施发布了问卷或面对面交流沟通，通过问卷调查和人员访谈收集到相关信息后，可以分析出安全管理方面的建设现状及佐证安全技术建设的效果。

2.2.1.3威胁评估

威胁是指可能对资产或用户组织造成损害事故的潜在原因。作为安全风险评估的重要因素，威胁是一个客观存在的事物，无论对于多么安全的信息系统都存在。威胁可能源于对用户组织直接或间接的攻击，例如非授权的泄露、篡改、删除等，对资产的保密性、完整性、可用性等方面造成损害。

用户需要对要保护的每一项关键信息资产进行威胁的识别。需要注意的是威胁总是不断变化的，尤其是业务环境与信息系统发生变化时。分析用户信息系统存在的威胁种类，确定威胁分类的标准；综合威胁来源、种类和其他因素后得出威胁列表；针对每项需要保护的信息资产，尽可能全面的发现资产所面临的威胁。

访谈调研：通过人员访谈方式与重要资产的所有人或管理人员面对面交流，直接获得重要资产曾经遭受过哪些具体威胁的破坏，或对一些安全事件表面现象进行分析后，间接获得安全事件背后的威胁源头。

人工审核：通过查看相关服务器的安全日志、往年的风险评估报告及等级保护测评书、以及应急响应报告等方面的文档数据，从中发现攻击、入侵或非法访问等威胁信息。

2.2.1.4风险分析

风险是一种潜在的可能性，是指某个威胁利用脆弱性引起某项资产或多项资产的损害，从而直接或间接的引起用户业务战略受损，因此风险和资产、威胁、脆弱性等因素息息相关。综合考虑资产本身的价值、威胁发生几率、脆弱性的破坏力、现有防护能力等因素分析资产可能存在的安全风险，结合风险对业务战略的影响程度区别是否可以接受。

2.2.1.5风险评估报告

根据资产识别、脆弱性评估、威胁评估、防护能力评估的输出结果进行风险分析之后，输出风险评估报告，风险评估报告中为用户提供符合业务需求的安全整改建议，从多角度多维度整改存在的安全问题，将用户的安全水平提升至更高的层次，尽量避免风险的重复性出现，保障业务系统安全可靠运行。

2.2.2服务范围

风险评估服务范围为温江区电子政务外网的云平台、网络设备、安全设备、中间件、数据库等信息化资产。1次/季度。

2.2.3服务成果

《风险评估报告》

2.3系统漏洞渗透测试服务

2.3.1服务内容

渗透测试是完全模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节，能够直观的让管理人员知道自己业务及网络所面临的问题。

渗透测试包括但不限于以下内容：

（1）身份验证类测试

用户注册：检查用户注册功能可能涉及的安全问题；

用户登录：检查用户登录功能可能涉及的安全问题；

修改密码：检查用户修改密码功能可能涉及的安全问题；

密码重置：检查忘记密码、找回密码、密码重置功能可能涉及的安全问题；

验证码绕过：检测验证码机制是否合理，是否可以被绕过；

用户锁定功能：测试用户锁定功能相关的安全问题。

（2）会话管理类测试

Cookie重放攻击：检测目标系统是否仅依靠cookie来确认会话身份，从而易受到cookie回放攻击

会话令牌分析：Cookie具有明显含义，或可被预测、可逆向，可被攻击者分析出cookie结构

会话令牌泄露：测试会话令牌是否存在泄露的可能

会话固定攻击：测试目标系统是否存在固定会话的缺陷

跨站请求伪造：检测目标系统是否存在CSRF漏洞

（3）访问控制类测试

功能滥用：测试目标系统是否由于设计不当，导致合法功能非法利用

垂直权限提升：测试可能出现垂直权限提升的情况

水平权限提升：测试可能出现水平权限提升的情况

（4）输入处理类测试

SQL注入：检测目标系统是否存在SQL注入漏洞

文件上传：检测目标系统的文件上传功能是否存在缺陷，导致可以上传非预期类型和内容的文件

任意文件下载：检测目标系统加载/下载文件功能是否可以造成任意文件下载问题

XML注入：测试目标系统-是否存在XML注入漏洞

目录穿越：测试目标系统是否存在目录穿越漏洞

SSRF：检测目标系统是否存在服务端跨站请求伪造漏洞

本地文件包含：测试目标站点是否存在LFI漏洞

远程文件包含：测试目标站点是否存在RFI漏洞

远程命令/代码执行：测试目标系统是否存在命令/代码注入漏洞

反射性跨站脚本：检测目标系统是否存在反射型跨站脚本漏洞

存储性跨站脚本：检测目标系统是否存在存储型跨站脚本漏洞

DOM-based跨站脚本：检测目标系统是否存在DOM-based跨站脚本漏洞

服务端URL重定向：检查目标系统是否存在服务端URL重定向漏洞

（5）信息泄露类测试

error code：测试目标系统的错误处理能力，是否会输出详尽的错误信息

Stack Traces：测试目标系统是否开启了Stack Traces 调试信息

敏感信息：尽量收集目标系统的敏感信息

（6）第三方应用类测试

中间件：测试目标系统是否存在jboss、weblogic、tomcat等中间件

CMS：测试目标系统是否存在dedecms、phpcms等CMS

2.3.2服务范围

温江区电子政务外网核心业务系统，每年2次。

2.3.3服务成果

《XX系统渗透测试报告》

2.4应急演练服务

2.4.1服务内容

根据相关国家标准或国际标准，提供对应的应急演练场景专项应急预案模板，以指导应急响应团队应对与处置安全事件；

制定应急演练方案及脚本并协助开展应急演练，模拟安全事件发生及处置的全过程，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。

应急演练服务主要通过模拟各种突发事件场景进行，根据突发网络安全事件的性质，应急演练场景可分为：有害程序事件演练、网络攻击事件演练、信息破坏事件演练、设备设施故障演练；

有害程序事件：内网传播型病毒应急演练、勒索病毒应急演练、挖矿病毒应急演练等；

网络攻击事件：漏洞攻击应急演练、后门攻击应急演练等；

信息破坏事件：网站篡改应急演练、网页挂马应急演练等；

设备设施故障事件：网络设备故障应急演练、服务器故障应急演练等

应急演练工作流程主要包括演练准备、演练实施、演练总结三个主要阶段

演练准备：主要包括需求调研、预案分析、演练场景设计、确定演练组织架构、演练方案制定、演练动员和培训、人员场地保障、演练工具保障及演练环境搭建；

演练实施：主要包括系统准备、演练启动、演练执行、演练解说、演练记录、演练结束及系统恢复；

演练总结：主要包括演练总结报告、文件归档备案、完善预案并提供改进建议。

通过提前制定应急演练预案，并协助单位开展预案演练，提高应对安全事件的处置能力，预防和减少安全事件造成的危害和损失。

2.4.2服务次数

每年1次

2.4.3服务成果

《应急演练报告》

2.5政务安全运营服务

7*24h安全运营服务

政务安全运营服务建设于电子政务外网内，依托政务外网向广大政务客户提供以保障网络安全“持续有效”为目标，围绕资产、漏洞、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式7*24小时持续性开展网络安全保障工作，与温江区电子政务外网一同构建持续（7*24小时）、主动、闭环的安全运营体系，帮助温江区电子政务外网实现风险可控、能力提升、价值可视。具体服务内容包括如下：

服务阶段	服务内容		
	服务项	服务细项	服务描述
	资产	资产发现与识别	借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保安全运营中心中资产信息的准确性和全面性。

			运营成熟度评估	识别与梳理	资产信息梳理与管理	结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息进行确认与更新。
				安全现状评估	脆弱性评估	系统与Web漏洞扫描：对操作系统、数据库、常见应用/协议、Web通用漏洞与常规漏洞进行漏洞扫描。
						弱口令扫描：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等
						基线配置核查：检查支撑信息化业务的主机操作系统、数据库、中间件的基线配置情况，确保达到相应的安全防护要求。检查项包含但不限于帐号和口令管理、认证、授权策略、网络与服务、进程和启动、文件系统权限、访问控制等配置情况
					病毒类事件评估	勒索病毒事件分析：安服专家分析判断主机是否感染了勒索病毒；是否已感染勒索病毒文件；根据已发生的漏洞攻击行为分析判断否存在勒索病毒攻击等。
						挖矿病毒事件分析：安服专家分析是否感染了挖矿病毒/木马；是否处于挖矿状态；根据已发生的漏洞攻击行为分析判断是否存在以植入挖矿木马为目的的漏洞攻击等
						蠕虫病毒事件：安服专家确认文件是否被感染，定位失陷的代码并进行修复
					攻击行为评估	针对漏洞利用攻击行为、Webshell上传行为、Web系统目录遍历攻击行为、SQL注入攻击行为、信息泄露攻击行为、口令暴力破解攻击行为、僵尸网络攻击行为、系统命令注入攻击行为及僵尸网络攻击行为进行分析评估，判断攻击行为是否成功以及业务风险点。
					失陷类事件评估	失陷主机分析：安全专家对失陷主机进行分析研判（如后门脚本类事件），并给出修复建议。
						潜伏威胁分析：安全专家分析内网主机的非法外联威胁行为，判断是否存在潜伏威胁，并给出解决建议。含：对外攻击、APT C&C通道、隐藏外联通道等外联威胁行为。
				问题处置	脆弱性问题处置	针对内网脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建议。
					病毒类事件处置	针对病毒类事件。安全专家提供病毒处置工具并主导查杀10个实例。若超过10个实例，安全专家固化出实际可行的措施，确保用户可进行查杀病毒。
					入侵攻击行为处置	针对分析研判确认的入侵行为，安全专家给出策略调整建议。
					失陷类事件处置	针对勒索、挖矿类事件。安全专家主导处置工作，并提供最大程度溯源服务（如涉及到重装业务系统，提供重装指导）；安全专家定位恶意文件路径并提供查杀指导（授权情况下，可由我方直接操作）；并分析有无异常进程与服务，发现异常进行通告（授权情况下，可由我方直接对异常情况进行操作）。
						针对后门脚本类事件。安全专家主导处置工作，提供专杀工具对感染服务器进行全面后门脚本查杀，并提供最大程度溯源服务。

					针对隐藏通信通道、可疑外发行为。安全专家提供实际佐证材料，并给出修复建议，提供最大范围的溯源服务。配合定位异常进程以及恶意文件，并提供查杀建议（客户授权情况下，我方开展查杀工作。默认主导查杀10个实例，若超过10个实例，固化出实际可行的措施，确保用户可进行查杀病毒。）
			运营能力评估	安全调查	采用线上调查问卷的方式，调研用户是否具备资产管理、漏洞管理、威胁监测技术、风险评估、应急预案等方面的信息安全措施。
				安全运营能力成熟度评估	采用线下访谈的方式，对用户信息安全措施进行调研评估。内容包含管理策略、资产管理、漏洞管理、威胁监测、威胁情报、风险评估、应急预案管理、安全事件管理。并根据调研的内容输出安全运营能力成熟度。
				安全运营能力成熟度解读	结合评估出的安全运营能力成熟度以及客户业务，提供安全能力差距分析报告解读。
			漏洞管理	漏洞分析与管理	漏洞扫描与验证：每月针对服务范围内的资产的系统漏洞和Web漏洞进行全量扫描，并针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。 每日针对变更的资产执行增量扫描，并针对发现的漏洞进行验证。
					漏洞修复优先级排序与通告：基于漏洞扫描结果、资产重要性及漏洞的威胁情报，对漏洞进行重要性排序，确定修复的优先级；并将最终结果通告给用户
					漏洞落地性处置建议：对漏洞进行分类并书写漏洞分类处置方案，并通过工单系统跟踪修复情况。
					漏洞复测与状态追踪：对修复的漏洞进行复测，关闭正常修复的漏洞的工单。制定漏洞闭环服务报告，并向管理层进行汇报
				弱口令分析与管理	实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。 针对不同行业提供行业密码字典，有针对性的进行内网弱口令检测。 并将检测发现的问题通过工单系统跟踪修复状态。
				最新漏洞预警与响应（可选）	资产指纹信息梳理：梳理信息化资产详情（含操作系统、中间件、数据库、应用框架，开发语言等指纹信息）并将梳理的信息录入安全运营平台。
					最新漏洞预警与排查：实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。
					最新漏洞处置指导：一旦确认漏洞影响范围后，安全专家提供专业的处置建议，处置建议包含两部分，补丁方案以及临时规避措施。
					最新漏洞复测与状态跟踪：由安全专家对该最新漏洞建立状态追踪机制；跟踪修复状态，遗留情况。
				漏洞协助处置	制定处置方案：根据用户实际业务场景需求，制定最适合的漏洞处置方案。
					处置方案验证：根据漏洞处置方案，在用户提供的测试环境中开展漏洞处置方案验证工作，观察处置方案对测试环境产生的影响，并提供最优修复方案建议。
					漏洞处置实施：在用户授权下，对漏洞进行处置工作，并验证漏洞是否依然存在以及配合验证业务影响面。

	1	持续有效运营	威胁管理	威胁分析与通告	结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态,发现各类安全事件，并自动生成工单
					实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。攻击事件包含域外黑客攻击事件、高级黑客攻击事件、持续攻击事件。
					实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发DOS型、C&C访问型、文件感染型、木马型。
					安全专家针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户
				流行威胁通告与排查	结合威胁情报，安全专家排查是否对用户资产造成威胁并通知用户，协助及时进行安全加固
				主动分析与响应	每月主动分析病毒类的安全事件：安全专家提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒；
					每月主动分析攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议。
					每月主动分析漏洞利用类的安全事件并验证该漏洞是否利用成功，提供工具协助处置；
					每月主动分析失陷类的安全事件并协助用户处置，并提供溯源服务
				策略管理	策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新
					策略定期管理：安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。
					策略调整：安全专家根据安全事件分析的结果以及处置方式，按实际要求对安全组件上的安全策略进行调整工作。
				持续攻击对抗	通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗。
					通过全网大数据分析，发现有域外黑客或高级黑客正在攻击，立即采取行动封锁黑客行为。
			事件管理	事件分析与处置	对用户上报的安全事件进行及时响应。
					实时针对异常流量分析、攻击日志和病毒日志分析，经过海量数据脱敏、聚合发现安全事件。
					针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助客户快速恢复业务，消除或减轻影响。
					入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务。

		应急响应	入侵威胁清除：排查攻击路径，恶意文件清除。
			入侵原因分析：还原攻击路径，分析入侵事件原因。
			加固建议指导：结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。
	运营可视	安全运营可视化	通过安全运营平台，随时查看业务资产安全状态。
			在线展示所有事件监测结果、防御过程和防御结果。
			在线展示所有服务内容、流程和事件处理进展。
		定期安全运营汇报	定期总结阶段性安全运营情况发送给用户，并向用户总结汇报。

2.5.2网站安全监测服务

网站安全监测服务是通过安全预警监测平台对WEB网站进行监测。安全预警监测平台集网站风险评估服务、实时监测服务、告警服务、威胁情报库、安全专家7*24小时值守等内容于一体化的强大的云端安全监测系统。平台应采用分布式架构部署，支持扫描器横向扩展，满足扫描吞吐量快速扩张的需求。系统应采用高可用设计，扫描执行服务器临时增（横向扩展）减（临时掉线）不会影响到扫描结果。扫描任务分发支持可靠性检测机制，确保任务不丢失。

网站管理员只需关注安全服务微信公众号可在线申请安全评估及监控服务，并通过公众号绑定的账号查收安全评估系统推送的安全事件报告，也可通过邮件告警，定期邮件形式推送安全报告到客户端。

网站安全监测服务应包括：网站风险评估服务、网站实时监测服务和及时告警服务。

风险评估风险监测平台自动化完成目标网站基线配置数据采集、基于网站特点的检测插件调度、目标网站响应数据处理过程，完成检测数据的智能统计分析后生成安全评估报表。

暴露面检测：通过对网站IP、操作系统版本、服务和端口、子域信息等进行信息收集和扫描，完成目标网站资产数据和基线配置信息的收集。

脆弱性检测：基于“暴露面检测”结果，智能调度仿攻击负荷（payload）的检测插件检测安全威胁。覆盖“信息泄露”、“配置隐患”、“SQL注入”、“XSS注入”等通用安全漏洞以及各种建站服务器、电子邮件系统、办公自动化系统漏洞及常见建站框架及建站语言漏洞。

内容安全检测：支持“暗链”和“敏感词”检测，基于机器学习算法帮助目标网站及时发现篡改隐患和内容违规风险。

实时监测服务针对影响网站运行和网站管理者声誉的重大隐患进行实时监控。覆盖网站页面篡改、挂马、黑链、可用性、内容安全、紧急漏洞的实时监控，确保管理员在网站发生如下情况时能及时得到通知并获得应急安全响应技术支持。

可用性监控：周期性发送PING、HTTP等请求检测网站是否可用；

内容安全监控：针对网站是否存在暗链篡改、DNS篡改、网站内容篡改、网站挂马以及网站内容中的反动、色情等非法的敏感词进行监控

紧急漏洞监控：对于漏洞攻击代码泄露；通用性框架的漏洞；厂商尚未发布补丁，或补丁发布时间<=30天；漏洞已经被较大规模（国外/国内）利用来进行攻击，具有较大影响；这类漏洞安全云平台会进行实时监控，及时发现风险。

及时告警服务通过微信公众号开始安全评估及监控服务，并通过公众号绑定的账户查收安全评估系统推送的安全事件报告。针对网页篡改、oday等紧急事件第一时间电话主动通知。

本次网站安全监测服务要求对温江区多个重要的网站进行安全监测服务。主要需监测的网站如：成都市温江区人民政府网站、信用中国（成都温江）、温江区政务服务网。交付的网站安全报告清单及交付方式如下：

交付文档	交付形式
网页篡改事件安全报告	微信
紧急漏洞事件安全报告	微信
黑链事件安全报告	微信
可用性安全报告	微信
安全评估报告	微信

2.5.3服务范围

主要服务包括温江区电子政务外网核心重要资产进行365天*24h持续安全保障，对10个网站进行网站安全监测服务。

2.5.4服务成果

《安全运营服务项目启动汇报PPT》

《客户启动会会议纪要》

《资产信息确认表》

《漏洞清单》

《漏洞举证报告》

《漏洞修复方案》

《首次安全分析与处置报告》

《首次上门处置问题记录表》

《安全运营问题跟踪处置列表》

《XXX安全威胁通告》

《XX事件应急响应报告》

《安全运营问题整改建议》

《安全运营周报》

《安全运营月报》

《安全运营季度报告》

《年度安全运营总结报告》

2.6重要时期保障服务

2.6.1服务介绍

为响应特殊时期客户业务系统的信息安全应急保障需求，提供短期的信息安全检查结合7*24小时值守的方式为客户的业务系统在特殊时期保驾护航。

2.6.2服务内容

在重大活动期间（如两会、国庆等）或重大网络安全事件期间提供现场安全值守服务，提供具有丰富的应急处理能力和安全服务技术经验的工程师。

服务内容包含如下内容：

制度符合性审查

网站7*24小时托管

威胁分析与处置

7*24小时驻点服务

应急响应

2.6.3服务周期

线上值守：在重保期间7*24h线上专家值守，每2h进行主动威胁狩猎并通报。

线下值守：在重保期间7*24h安全服务工程师驻场。

2.6.4服务范围

温江区电子政务外网所属资产。

2.6.5服务交付

对客户的重要时期服务所提交的交付物不限于以下：

《网络安全监测服务日报》

《网络安全预警通报周报》

《重要时期保障值守总结》

2.7安全培训服务

依据温江区电子政务外网需求提供针对性的安全培训。可根据客户需求进行定制，例如针对IT部门□员开展技能培训、为企业员□提供安全意识培训等，培训时长视培训内容□定。

2.7.1服务内容

（1）安全意识培训

针对安全意识等信息提供培训服务，使被培训者通过学习了解到当前网络存在的安全风险和隐患，提升客户非技术人员的整体安全意识和安全防护能力。

安全技能培训

（2）针对安全攻防、漏洞挖掘、应急响应、安全运维等提供培训服务，使被培训者通过学习了解到漏洞挖掘、应急响应的思路和方法，达到能够独立实施常规的安全工作，从根本上帮助客户提高安全能力。

2.7.2服务流程

（1）前期准备

与客户确定培训需求、确定培训方案、确定培训方式，根据客户要求完成课件编写。

（2）实施培训

按照前期确定信息开展培训工作，进行授课讲解及培训效果评估。

（3）成果汇报

对培训工作进行复盘总结。

2.7.3服务交付物

《安全培训PPT》

2.8安全管理制度服务

本期安全管理制度建设主要有以下几个方面：

制定安全管理制度和配套的发布、评审和修订机制；

（1）人员管理

包括配套的培训和考核机制。需要建立内部人员管理制度和外部人员管理制度，包括：

内部工作人员管理

正式编制人员，聘用人员等人员的录用、岗位职责、保密协议签证、教育培训、保密监管、奖惩和离岗离职的管理。

外部相关人员管理

内部工作人员之后的其他人员以及设备（特别是进口设备）的维修服务人员等外来人员的保密要求知会、安全控制区域隔离、携带物品限制和旁站陪同控制。

（2）物理环境与设施管理

建立物理环境与设备管理制，包括：

周边环境：包括周边监制、周界安防和出入控制。

涉密场所：包括保密要害部门部位管理、无线产品使用、多媒体产品使用和安全巡防巡查、窃密（窃听、窃照、窃收等）检查。

保障设施：包括定期检测检修和线路线缆保护。

（3）设备与介质管理

建立设备与介质管理制度，包括：

设备与介质的采购与选型：安全采购管理、产品选型管理、检测证书查验和货物交付验收。

设备与介质的操作与使用：安全操作使用、外出携带管理、设备外联控制、介质使用管理、安全准入许可。

设备与介质的保存与保管：清查登记核对、重要设备办公室和明确责任主体。

设备与介质的维修与报废：申报审批、数据保护和登记备案。

（4）信息保密管理

建立信息保密管理制度，包括：

信息分类与控制：密级分类确定、密级信息问题统计、密级标识添加和知悉范围确定。

管理与授权：清单管理、标识符管理和权限列表审查。

信息系统安全互联控制。

2.8.1安全管理机构

本期安全管理机构建设主要有以下几个方面：

设定安全管理员一职,并明确岗位的职责与任务，落实安全管理责任制。

2.8.2人员安全管理

本期人员安全管理建设主要有以下几个方面：

聘请专业咨询公司，制定安全培训管理方案，制度化、常态化进行安全培训。

进一步规范人员录用、人员离岗、人员考核、外部人员访问的管理制度。

对温江区电子政务外网工作人员进行安全意识培训，加强人员安全意识、避免安全管理漏洞。

2.8.3系统建设管理

本期系统建设管理主要有以下几个方面：

制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等内容的管理责任部门、具体管理内容和控制方法，并按照管理制度落实各项管理措施。

2.8.4系统运维管理

本期系统运维管理主要有以下几个方面：

对系统的环境和资产安全、设备和介质安全、网络安全、系统安全、备份与恢复等进行管理和定期维护。

2.8.5云计算中心运维管理

2.8.5.1维护组织架构及职责分工

确定政务云平台的资源池的维护单位职责、云平台上所承载的业务平台的维护单位职责、确定政务云平台资源可申请单位范围。

确定云计算后新增的维护岗位职责：云平台资源管理员、云平台服务管理员、云平台安全管理员、云平台统计分析员角色。

2.8.5.2制定规章制度

协助制定以下管理制度：

资源申请：申请人资格、申请时需要提交的材料、审核环节的设定等

资源回收：申请人资格、申请时需要提交的材料、审核环节的设定等

资源配置调整：申请人资格、需要提交的申请材料、审核环节的设定等

资源下线：申请人资格、申请时需要提交的材料、审核环节的设定等

故障处理：各方责任确立

2.9安全咨询规划服务

结合温江区电子政务外网实际情况，通过信息安全制度调研、资产清单、访谈调查等进行安全现状调研，在此基础上进行安全管理、安全技术体系差距分析，结合风险分析输出安全体系强度评估结果，最后进行信息安全体系规划。

主要工作内容如下：

2.9.1安全现状调研

在安全现状调研阶段，主要是通过问卷调查、现场访谈、文件审核等方式对单位安全现状进行调查，摸清组织安全现状。

（1）信息安全管理制度调研

针对单位当前的信息安全管理制度进行详细调研，以了解当前管理制度上是否存在缺陷，是否需要进行优化改进。

（2）资产清单梳理

针对单位关键业务系统进行资产梳理核对，形成资产配置清单，包括但不限于：

机房信息调研

业务系统调研

虚机、实体机情况情况调研

网络设备调研

安全物理环境调研

安全区域边界调研

安全计算环境调研

安全管理中心调研

2.9.2安全体系强度评估

（1）安全管理体系差距评估

通过现场访谈方式，针对单位当前安全管理制度、管理流程进行差距分析。

信息部门安全访谈-高层管

信息部门安全访谈-中层管理

信息部门安全访谈-应用运维岗位

信息部门安全访谈-开发岗

信息部门安全访谈-信息安全管理员

信息部门安全访谈-物流IT高级经理

信息部门安全访谈-机房管理员

人资部门安全访谈

最终，根据访谈结果进行汇总梳理，输出单位当前安全管理体系调研报告。

（2）安全技术体系差距评估

针对单位当前的安全业务现状，对相关设备进行差距分析。

网络设备基线核查

业务系统基线核查

虚拟机及实体机基线核查

（3）安全风险分析

针对单位当前的安全业务现状，采用信息安全风险评估的方法，对系统、设备进行全面的脆弱性、威胁和业务风险等方面进行系统化的测评分析，发现基于业务的安全风险问题。

业务系统基线核查

渗透测试

漏洞扫描

系统代码审计

2.9.3安全蓝图规划

从增强技术体系、完善管理体系等方面制定完整的安全保障体系规划，拟定可执行的实施计划。

2.9.3.1信息安全技术体系设计

以安全理论模型为依据，依据等级保护等标准，设计覆盖核心业务系统，规划建立起保护、检测和响应的安全技术防护体系，并遵照纵深防御的思想将安全防护措施覆盖到信息安全技术的各个层面，可有效抵御各类信息安全威胁的技术体系。

分域保护框架规划

根据业务系统的安全需求，遵循安全域划分的原则，可以对现有网络系统进行规划、梳理，最终形成以安全域为模块的网络结构。

通过划分安全域的方法，将网络系统按照业务流程的不同层面划分为不同的安全域，各个安全域内部又可以根据业务元素对象划分为不同的安全子域。针对每个安全域或安全子域来标识其中的关键资产，分析所存在的安全隐患和面临的安全风险，然后给出相应的保护措施；不同的安全子域之间和不同的安全域之间存在着数据流，需要实施安全域边界的访问控制、身份验证和审计等安全策略。

安全通信网络规划

从网络结构安全、网络安全审计、网络设备防护、通信完整性和通信保密性等几个方面，保证安全通信网络通信过程中数据的完整性、保密性和通信过程的可靠性。

（1）网络结构安全

网络结构的安全是网络安全的前提和基础，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机；合理规划路由，业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各业务系统的重要性和所涉及信息的重要程度等因素，划分不同的网段或VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

（2）网络安全审计

网络安全审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的安全事件，包括各种外部事件和内部事件。可在各网络区域部署威胁探针流量分析设备或防火墙设备，对网络内的数据包进行全量还原，记录各类TCP/UDP协议日志，形成对全网网络数据的流量监测并进行相应安全审计，同时和其它网络安全设备共同为安全管理中心提供监控数据用于分析及检测。

威胁探针流量分析设备将独立的网络传感器硬件组件连接到网络中的数据会聚点设备上，对网络中的数据包进行分析、匹配、统计，通过特定的协议算法，从而实现网络审计功能。威胁探针流量分析设备采用旁路技术，不用在目标主机中安装任何组件。同时流量分析设备可以与其它网络安全设备进行联动，将各自的监控记录送往安全管理中心，集中对网络异常、攻击和未知威胁等进行分析和检测。

（3）网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的加固措施。对于

网络中关键的交换机、路由器等网络设备，也需要采用一定的安全设置及安全保障手段来实现网络层的控制。

（4）通信完整性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。对于信息传输的完整性校验应由传输加密系统完成。

（5）通信保密性

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，并对通信过程中的敏感信息字段进行加密。

（6）网络可信接入

为保证网络边界的完整性，不仅需要进行非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。网络可信接入一般是对用户终端进行控制，可通过终端安全准入系统实现重点终端的可信接入。

安全计算环境规划

计算环境是应用系统的运行环境，包括应用系统正常运行所必须的终端、服务器、网络设备等，计算环境安全是应用系统安全的根本。一个安全的计算环境可以有效防止非授权用户访问和授权用户越权访问，为应用系统的正常运行和免遭恶意破坏提供支撑和保障。因此，安全计算环境主要是重点加强系统数据库的审计建设，确保信息和信息系统的机密性和完整性。

安全计算环境的规划将依照身份鉴别、访问控制、安全审计、入侵防范、主机恶意代码防范、软件容错、数据完整性与保密性、软件容错、备份与恢复、资源控制、客体安全重用和抗抵赖等方面进行设计。

安全区域边界规划

区域边界是应用系统运行环境的边界，是应用系统和外界交互的必经渠道，通过区域边界的安全控制，可以对进入和流出应用环境的信息流进行安全检查，既可以保证应用系统中的敏感信息不会泄漏出去，同时也可以防止应用系统遭受外界的恶意攻击和破坏。因此，安全区域边界规划主要是重点合理的划分区域、区域隔离，通过高性能UTM强化访问控制策略和网络边界的防病毒。

安全区域边界的规划将以下几个方面，加强安全区域边界的防攻击能力：

从边界访问控制

边界入侵防范

边界恶意代码防范

流量控制

安全审计

边界完整性检查

2.9.3.2信息安全管理体系设计

以实际情况和现实问题为基础，依据等级保护等标准，在满足政策的基础上针对温江区电子政务外网制定信息安全方针与信息安全目标，完善信息安全管理体系，形成完整的安全管理框架结构。安全管理体系主要包括安全管理机构、安全管理制度、安全管理人员、安全建设管理、安全运维管理几个方面。

安全管理机构

为保障信息安全工作落到实处，应重新梳理安全管理组织，形成由业主单位牵头的信息安全小组、具体信息安全职能部门负责日常工作的组织模式。

为了有效落实信息安全各项工作，应设立以下专职的安全岗位，负责安全工作的落实和执行：

（一）信息安全工作组主管

负责网络与信息安全的日常整体协调、管理工作；

负责组织人员制定信息安全管理制度，并对管理制度进行推广、培训和指导；

负责重大安全事件的具体协调和沟通工作。

（二）安全管理员岗位

负责执行网络与信息安全工作的日常协调、管理工作；

负责日常的安全监控管理，并对上报和发现的各类安全事件进行处置；

负责系统、网络和应用安全管理的协调和技术指导；

负责安全管理平台安全策略制定，访问控制策略审核；

负责组织安全管理制度的推广和培训工作；

负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

（三）安全审计员岗位

负责安全管理制度落实情况的检查、监督和指导；

负责安全策略执行情况的审核。

（四）系统管理员

负责系统安全稳定运行的日常管理工作；

负责保持系统的防病毒系统、补丁等保持最新，定期对系统进行安全加固，保持系统漏洞最小化。

（五）网络管理员

负责网络设备安全稳定运行的日常管理工作；

负责保持网络设备的漏洞最小化，定期对系统进行安全加固；

负责保持网络路由和交换策略与业务需求保护一致。

根据日常的运行维护和管理工作，设置物理环境管理、业务管理、应用管理以及资产管理等岗位，这些岗位也应当包括安全职责，这些安全职责的具体内容通过《信息安全管理岗位说明书》落实。

安全管理制度

针对当前安全管理制度进行系统性梳理，建立信息安全方针、安全策略、安全管理制度、安全技术规范以及流程的一套信息安全管理制度体系。

安全管理制度建设框架

（1）安全方针和主策略

制定网络安全工作的最高方针，作为纲领性的安全策略主文档，需要陈述本策略方针的目的、适用范围、信息安全的管理意图、支持目标以及指导原则，信息安全各个方面所应遵守的原则方法和指导性策略。

（2）安全管理制度和规范

从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是必须具有可操作性，而且必须得到有效推行和实施的。

技术标准和规范，包括各个安全等级区域网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。根据实际需求调研情况，梳理出如下安全管理制度和规范需求目录：

安全方针

安全策略

安全管理组织体系职责

内部人员安全管理规定

外部人员安全管理规定

风险评估管理规范

软件开发管理规定

IT外包管理规定

工程安全管理规定

产品采购安全管理规定

服务商安全管理规定

机房管理制度

办公环境安全管理规定

资产安全管理制度

设备安全管理规定

介质安全管理规定

运行维护安全管理规范

网络安全管理规定

系统安全管理规定

防病毒安全管理规定

密码使用管理制度

变更管理制度

备份与恢复管理规定

安全事件管理制度

应急预案

（1）安全流程和操作规程

详细规定主要业务应用和事件处理的流程和步骤，以及相关注意事项。作为具体工作时的具体依照，此部分必须具有可操作性，而且得到有效推行和实施。

（2）安全记录单

落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

（3）安全管理制度体系文件管理

安全策略系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

人员安全管理

（1）内部人员安全管理

主要是指针对内部人员的安全管理，从人员的录用、调用、离岗和考核等各个方面提出针对信息安全的相关管理要求。

（2）外部人员安全管理

外部人员通常是指软件开发商，硬件供应商，系统集成商，设备维护商，和服务提供商，实习生，临时工等非内部人员。外部人员在访问时可以分成物理访问和信息访问进行安全管理。

（3）安全教育培训和体系宣贯

根据用户的不同层次制定相应的教育培训计划及培训方案，并在教育培训的过程中融合信息安全体系的内容对员工进行体系的宣贯，主要包括：安全培训教育、安全活动、安全宣传等三个方面。

为了将安全隐患减少到最低，不仅需要对安全管理员进行专业性的安全技术培训，还需要对一般办公人员的信

息安全意识进行教育和培训，普及信息安全基本知识，通过对用户的不断教育和培训，增强全体工作人员的信息安全意识、法制观念和技术防范水平，从安全工作的开展角度来看，提升全体人员的信息安全意识和技能有利于安全工作的顺利开展和安全效果的有效保证，更高效地全面地达到安全建设目标。

安全建设管理

（1）等级保护信息系统建设安全管理

根据等级保护的要求，作为安全建设的指导性文件，信息系统安全建设遵循《信息系统安全保护等级实施指南》和《网络安全等级保护基本要求》，安全建设管理中的定级与备案、安全方案设计和等级测评等方面的要求也将主要依据以上标准的最新要求为准进行，需要明确每一阶段工作的相关责任人和具体流程。

（2）统建设安全管理规划设计

在系统建设方面，在新建信息系统或信息系统变更的时候，需要从系统立项、方案设计、采购、开发、测试、验收、交付、使用等方面进行规划。

安全运维管理

按照等级保护要求和现状分析，日常运维管理主要从以下九个方面进行考虑。

环境管理

资产管理

网络安全管理

系统安全管理

防病毒管理

管理和安全管理中心

密码管理

变更管理

备份与恢复管理

根据国家信息系统等级保护和行业有关要求，结合温江区电子政务外网自身的实际情况，分别从人员技能考核、各部门信息安全工作情况等方面进行考核规划设计，全面考察各部门安全管理和技术水平。

（1）人员技能考核

根据国家信息系统等级保护和行业有关要求，在人员技能考核方面的规划内容如下：

定期对各个岗位的人员进行安全技能及安全认知的考核，如可通过理论考试等方式；

对关键岗位的人员进行全面、严格的安全审查和技能考核，如通过安全实际操作的方式进行考核；

对考核结果进行记录并保存。

（2）信息安全工作考核

根据国家信息系统等级保护和行业有关要求，在信息安全工作考核方面的规划内容如下：

制定信息安全工作考核计划和方案；

信息安全工作考核计划包括：等保工作的开展情况、安全事件发生情况、上级单位政策的执行情况、安全漏洞整改情况等等；

每半年对信息安全工作情况进行一次考核；

考核方式可采取信息安全自查和抽查的方式，并根据打分制进行打分。

★	2	**二、人员配置要求** （1）需提供1名专职技术工程师常驻现场，协助我单位开展日常安全服务工作。 （2）需提供固定的7×24小时故障受理电话服务及工作日提供7×8小时的驻场服务。认真完做好本项目的安全服务包括安全服务评估、安全技术防范服务和安全运维服务。 （3）驻场工程师具有本科或以上学历，并且在计算机及其设备硬件技术、操作系统软件、常用应用软件、网络技术、安全技术、系统运行与维护工作管理方面具有非常专业的经验和知识，有相关工作经验3年以上。 （4）驻场工程师需接受我单位的管理，必须遵守我单位相关的规章制度及相关的保密规定，我单位对驻场工程师的表现不满意有权要求服务提供商更换。 （5）保证派驻到我单位的技术工程师的稳定性，未经甲方书面同意，不得随意更换驻场工程师。 （6）驻场工程师须自觉主动进行日常常规的巡检和维护保养工作。 （7）服务提供商还必须组建完整的项目组，除上述驻场运维服务人员外，须安排项目经理1人、技术负责人1人以及不小于4人的二线技术支持服务组，参与本项目的项目管理、技术支撑、日常巡检、突发事件、应急事件服务工作。并能根据一些特殊的情况可以适当增加运维服务人员。本项目的技术人员和项目负责人必须固定，如有变更，必须经我单位同意并签字确认。

3.2.3人员配置要求

采购包1：

（1）需提供1名专职技术工程师常驻现场，协助我单位开展日常安全服务工作。（2）需提供固定的7×24小时故障受理电话服务及工作日提供7×8小时的驻场服务。认真完做好本项目的安全服务包括安全服务评估、安全技术防范服务和安全运维服务。（3）驻场工程师具有本科或以上学历，并且在计算机及其设备硬件技术、操作系统软件、常用应用软件、网络技术、安全技术、系统运行与维护工作管理方面具有非常专业的经验和知识，有相关工作经验3年以上。（4）驻场工程师需接受我单位的管理，必须遵守我单位相关的规章制度及相关的保密规定，我单位对驻场工程师的表现不满意有权要求服务提供商更换。（5）保证派驻到我单位的技术工程师的稳定性，未经甲方书面同意，不得随意更换驻场工程师。（6）驻场工程师须自觉主动进行日常常规的巡检和维护保养工作。（7）服务提供商还必须组建完整的项目组，除上述驻场运维服务人员外，须安排项目经理1人、技术负责人1人以及不小于4人的二线技术支持服务组，参与本项目的项目管理、技术支撑、日常巡检、突发事件、应急事件服务工作。并能根据一些特殊的情况可以适当增加运维服务人员。本项目的技术人员和项目负责人必须固定，如有变更，必须经我单位同意并签字确认。

3.2.4设施设备配置要求

采购包1：

无

3.2.5其他要求

采购包1：

（1）服务提供商提供的服务工具应满足未来3年成都市温江区电子政务外网发展需要，符合招标文件中的相关要求。如服务提供商提供的服务工具及运维服务人员在服务过程中不能满足采购人要求，服务提供商应更换服务工具或运维服务人员。（2）服务工具可用性要求：服务提供商提供的服务工具可用性应不小于99.99%。（3）响应时间：出现故障或安全问题后响应时间小于15分钟。对于驻场工程师不能解决的问题，服务提供商应派专业的技术人员以最短时间赴现场分析原因，制定解决方案，最终解决问题，全部实际发生的费用由服务提供商承担（包括交通费和住宿费等）。处理时限见如下： 一级故障，立即响应，2小时内恢复； 二级故障，立即响应，4小时内恢复； 三级故障，立即响应 ，12小时内恢复. 服务提供商应在故障处理完毕后24小时内向采购人提交事件处理报告。

3.3商务要求

3.3.1服务期限

采购包1：

自合同签订之日起1095日

3.3.2服务地点

采购包1：

温江区人和路733号

3.3.3考核（验收）标准和方法

采购包1：

1.技术履约内容及标准： 服务提供商应针对本项目建立完善的质量管理体系，并配备相应的人员或机构，确保项目服务质量的落实和保证。 服务提供商应配合采购人按照采购人制定的服务考核指标定期对本项目各项服务进行质量考核。 服务质量主要指标。要求保证设备可用性不低于99.95%，年度服务费用结算将结合服务质量考核结果，按比例扣除相应服务费用。应用系统可用性=（365×24×60×60秒－单个应用失效时间之和（秒））/（365×24×60×60秒）；即：全年失效时间不超过365×24×60×0.0005=262.8分钟。应用失效时间指服务提供商提供的安全服务等方面出现的严重问题引起应用系统失效时间。经采购人认定由非供应商引起的系统失效（如不可抗力）不包含在内。 采购人有权对服务提供商的驻场人员的出勤率及技术水平进行考评，如果达不到要求，有权要求服务提供商更换驻场人员，直到采购人满意为止。 本项目中所有服务以签署验收报告作为验收标志，同时作为支付尾款的条件。 服务验收：服务提供商按时提交所有的提交物，各项服务水平达到要求后，进入验收流程。

3.3.4支付方式

采购包1：

分期付款

3.3.5.支付约定

采购包1： 付款条件说明： 本项目共有3个服务期，每个服务期为1年，合同1年1签。每个服务期到期后经考核合格后方可续签下一个服务期的服务合同 ，达到付款条件起 7 日内，支付合同总金额的 50.00%。

采购包1： 付款条件说明： 服务期开始后 ，达到付款条件起 7 日内，支付合同总金额的 40.00%。

采购包1： 付款条件说明： 1个服务期满后并经验收合格后 ，达到付款条件起 7 日内，支付合同总金额的 10.00%。

3.3.6违约责任与解决争议的方法

采购包1：

发出书面通知要求中标公司履行合同内容;如在通知限期内无法履行合同,发出解除合同通知，必要时要求对方承担违约责任;

3.4其他要求

无

第四章 资格审查

资格审查由 成都市温江区智慧蓉城运行中心和成都鑫源至成工程项目管理咨询有限公司 组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

4.1一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	具有独立承担民事责任的能力。	1、企业法人：提供“统一社会信用代码营业执照”（注：分公司参与项目磋商的，需提供总公司的有关文件或制度等能够证明总公司授权其独立开展业务的证明材料复印件。）； 2、事业法人：提供“统一社会信用代码法人登记证书”； 3、其他组织：提供“对应主管部门颁发的准许执业证明文件”或“统一社会信用代码的社会团体法人登记证书”或“统一社会信用代码的民办非企业单位登记证书”或“统一社会信用代码的基金会法人登记证书”； 4、个体工商户：提供“统一社会信用代码营业执照”； 5、自然人：提供“身份证明材料”。	投标人应提交的相关资格证明材料
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
3	具有健全的财务会计制度。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

4.2特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
无			

4.3落实政府采购政策资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包属于专门面向小微企业采购。	供应商需在项目电子化交易系统中按要求填写《中小企业声明函》并进行电子签章；供应商如属于残疾人福利性单位，需在项目电子化交易系统中按要求填写《残疾人福利性单位声明函》并进行电子签章；供应商如属于监狱企业，需在项目电子化交易系统中按要求上传监狱企业证明文件并进行电子签章。	中小企业声明函 残疾人福利性单位声明函 投标文件封面 监狱企业的证明文件

第五章 评标办法

5.1 总则

一、根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购货物和服务招标投标管理办法》等法律规章，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序和标准对待所有的投标人。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标文件规定和项目电子化交易系统操作要求开展或者参加评标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评标委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评标活动的，将依法追究其责任。

5.2评标委员会

一、本项目评标委员会成员人数应当为五人以上单数，其中评审专家不得少于成员总数的三分之二。评审专家是采取随机方式在采购一体化平台的专家库系统（以下简称专家库系统）抽取。技术复杂、专业性较强的采购项目，评审专家中应当包含1名法律专家。

二、评标委员会成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

（一）熟悉和理解招标文件；

(二)审查供应商投标文件等是否满足招标文件要求，并作出评价；

(三)根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出 澄清、说明或者更正；

(四)推荐中标候选供应商，或者受采购人委托确定中标供应商；

(五)起草评标报告并进行签署；

(六)向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；

(七)法律、法规和规章规定的其他职责。

5.3评标方法

采购包1：综合评分法

5.4评标程序

5.4.1熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项

目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

（一）招标文件的规定存在歧义、重大缺陷的；

（二）招标文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；

（三）采购项目属于国家规定的优先、强制采购范围，但是招标文件未依法体现优先、强制采购相关规定的；

（四）采购项目属于政府采购促进中小企业发展的范围，但是招标文件未依法体现促进中小企业发展相关规定的；

（五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；

（六）招标文件将投标人的资格条件列为评分因素的；

（七）招标文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评标情形的，评标委员会应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在四川政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

5.4.2符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。	开标一览表 分项报价表

2	投标文件是否满足招标文件规定的实质性要求	1、投标文件的格式、语言、计量单位、报价货币、知识产权、投标有效期等不符合招标文件的规定，影响评标委员会评判的。 2、投标报价不符合招标文件规定的报价要求的。 3、招标文件有明确要求，但投标文件未载明或者载明的采购项目履约时间、方式、数量与招标文件要求不一致的。4、针对招标文件第二章2.4.9中“投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应”，除招标文件中的明确要求进行单独响应或承诺的实质性要求外，对于其他实质性要求，供应商在《投标（响应）函》中以“我单位完全接受和理解本项目采购文件规定的实质性要求”进行承诺即视为响应。	实质性要求响应函
3	对商务要求响应的审查	招标文件中的商务要求，供应商应进行响应，没有进行响应但未标明是负偏离的，也视为完全满足。	商务应答表
4	法人授权书及法人身份证明	投标人提供法人授权书及法人身份证明。若投标人为自然人的可不提供。	法人授权书及法人身份证明

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

（一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；

（二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。

（三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

（一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（二）大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；

（三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

5.4.5复核

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选供应商、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

（一）分值汇总计算错误的；

（二）分项评分超出评分标准范围的；

（三）评标委员会成员对客观评审因素评分不一致的；

（四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

5.4.6确定中标候选人名单

采购包1：确定3家供应商为中标候选人。

（综合评分法适用）按投标人综合得分从高到低顺序排列，确定中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

（最低评标价法适用）按投标人投标报价从低到高顺序排列，确定中标候选人。投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

一、招标公告刊登的媒体名称、开标日期和地点；

二、投标人名单和评标委员会成员名单；

三、评标方法和标准；

四、开标记录和评标情况及说明，包括投标无效投标人名单及原因；

五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；

六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者更正，评标委员会成员的更换等；

七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由

的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

（综合评分法适用）采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。

投标报价得分=（评标基准价／投标报价）×100

评标总得分＝F1×A1＋F2×A2＋……＋Fn×An

F1、F2……Fn分别为各项评审因素的得分；

A1、A2、……An 分别为各项评审因素所占的权重（A1＋A2＋……＋An＝1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审100.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	投标报价	1、经评审委员会评审，有效投标报价最低的投标人的投标报价作为评标基准价； 2、投标报价得分=(评标基准价／投标报价)×报价分值。	10.00	客观	开标一览表 分项报价表
	商务评议	1、投标人具有有效质量管理体系认证证书得2分； 2、投标人具有有效信息安全管理体系认证证书得2分； 3、投标人具有有效信息技术服务管理体系认证证书得2分；（注：提供证书复印件并加盖供应商公章）	6.00	客观	投标人认为需要提供的其他证明材料

服务团队	1、投标人拟派本项目的项目经理具有①信息系统项目管理师（计算机技术与软件专业技术资格（水平）；②ITSS服务项目经理；③网络安全能力认证（CCSC）证书的，每有一项得2分，最多得6分。 2、投标人拟派本项目的技术负责人具有①网络安全服务类中级及以上职称；②信息系统项目管理师（计算机技术与软件专业技术资格（水平）；③ITSS服务项目经理；④注册信息安全专业人员（CISP）证书的，每有一项得3分，最多得12分。 3、投标人拟派本项目的驻场运维服务人员具有①信息化类中级及以上职称；②网络工程师（计算机技术与软件专业技术资格（水平）；③网络安全能力认证（CCSC）证书的，每有一项得2分，最多得6分。（注：1.提供证书复印件及该人员在投标人单位在职的在职证明材料并加盖投标人公章；2.项目经理、技术负责人与驻场运维服务人员须一岗一人，不可兼任。）	24.00	客观	投标人认为需要提供的其他证明材料
运维能力	投标人具有运维管理工具平台的得3分。（注：供应商提供运维管理平台相关计算机软件著作权登记证书并加盖公章）	3.00	客观	投标人认为需要提供的其他证明材料
履约能力	2020年1月1日后（含）投标人具有类似项目业绩，每有一个得1分，最多得2分。（注：1.类似项目是指信息安全运维服务或信息安全建设项目；2.须提供类似项目业绩合同复印件或成交（中标）通知书或成交（中标）公告截图。）	2.00	客观	投标人认为需要提供的其他证明材料

详细评审	技术评审	投标人提供本地驻场安全运维服务方案，内容包括但不限于：①资产管理；②安全巡检；③安全检查；④安全通告与预警；⑤应急响应服务。全部内容完整有效的得10分，每有一项缺失扣2分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣1分，扣完为止。	10.00	主观	投标人认为需要提供的其他证明材料
	技术评审	投标人提供安全风险评估服务方案，内容包括但不限于：①资产识别；②脆弱性评估；③威胁评估；④风险分析；⑤风险评估报告。全部内容完整有效的得10分，每有一项缺失扣2分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣1分，扣完为止。	10.00	主观	投标人认为需要提供的其他证明材料
	技术评审	投标人提供系统漏洞渗透测试服务方案，内容包括但不限于①服务内容；②服务范围；③服务成果。全部内容完整有效的得6分，每有一项缺失扣2分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣1分，扣完为止。	6.00	主观	投标人认为需要提供的其他证明材料
	技术评审	投标人提供应急演练服务方案，内容包括但不限于①服务内容；②服务次数；③服务成果。全部内容完整有效的得6分，每有一项缺失扣2分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣1分，扣完为止。	6.00	主观	投标人认为需要提供的其他证明材料

技术评审	投标人针对本项目提供政务安全运营服务方案，方案内容包括但不限于：①安全运营服务；②网站安全监测服务；③服务范围；④服务成果。全部内容完整有效的得8分，每有一项缺失扣2分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣1分，扣完为止。	8.00	主观	投标人认为需要提供的其他证明材料
技术评审	投标人提供重要时期保障服务方案，内容包括但不限于：①服务内容；②服务周期；③服务范围；④服务交付。全部内容完整有效的得4分，每有一项缺失扣1分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣0.5分，扣完为止。	4.00	主观	投标人认为需要提供的其他证明材料
技术评审	投标人提供安全培训服务方案，内容包括但不限于：①服务内容；②服务流程；③服务交付物。全部内容完整有效的得3分，每有一项缺失扣1分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣0.5分，扣完为止。	3.00	主观	投标人认为需要提供的其他证明材料
技术评审	投标人提供安全管理制度服务方案，内容包括但不限于：①安全管理机构；②人员安全管理；③系统建设管理；④系统运维管理；⑤云计算中心运维管理。全部内容完整有效的得5分，每有一项缺失扣1分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣0.5分，扣完为止。	5.00	主观	投标人认为需要提供的其他证明材料

	技术评审	投标人提供安全咨询规划服务方案，内容包括但不限于：①安全现状调研；②安全体系强度评估；③安全蓝图规划。全部内容完整有效的得3分，每有一项缺失扣1分；每有一处不满足招标文件要求或与整体服务方案矛盾或不符合实际情况或缺陷漏项或存在逻辑错误的扣0.5分，扣完为止。	3.00	主观	投标人认为需要提供的其他证明材料

价格扣除

序号	情形	适用对象	扣除比例(C1)	说明	关联格式
无					

说明：

1、评分的取值按四舍五入法，保留小数点后两位；

2、评分标准中要求提供的证明材料须清晰可辨。

（最低评标价法适用）采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标：

一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；

二、出现影响采购公正的违法、违规行为的；

三、投标人的报价均超过了采购预算，采购人不能支付的；

四、因重大变故，采购任务取消的；

废标后，代理机构将在四川政府采购网上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在倾向性和歧视性、是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定1名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

5.8.2定标程序

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起2个工作日内将评标报告送采购人。

三、采购人在收到评标报告后5个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在四川政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9评审专家在政府采购活动中承担以下义务

（一）遵守评审工作纪律；

（二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；

（三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；

（四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

（五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

（六）配合答复处理供应商的询问、质疑和投诉等事项；

（七）法律、法规和规章规定的其他义务。

5.10评审专家在政府采购活动中应当遵守以下工作纪律

（一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

（二）评标前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

（三）评标过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的， 应当在监督人员监督之下办理。

（四）评标过程中，不得干预或者影响正常评标工作，不得发表倾向性、引导性意见， 不得修改或细化招标文件确定的评标程序、评标方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评标意见，不得拒绝对自己的评标意见签字确认。

（五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，除因履行本规程第十三条第（六）项规定的义务外，不得向外界透露评审内容。

（六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

（七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

第6章投标文件格式

6.1投标文件封面格式

采购包1：

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标（响应）函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：投标人应提交的相关资格证明材料

详见附件：商务应答表

详见附件：开标一览表

详见附件：分项报价表

详见附件：投标人认为需要提供的其他证明材料

详见附件：法人授权书及法人身份证明

详见附件：实质性要求响应函

政府采购合同（服务类）

政府采购合同编号：_____

履约地点：_____

签订日期：20___年___月___日

签订地点：_____

采购人（甲方）：_____

地址：_____

供应商(乙方)：_____

地址：_____

依据《中华人民共和国民法典》《中华人民共和国政府采购法》与项目行业有关的法律法规，以及XXX采购项目的《采购文件》，乙方的《投标（响应）文件》及《中标（成交）通知书》，甲乙双方同意签订本合同。具体情况及要求如下

一、标的信息

二、服务要求

三、合同定价方式、付款进度和支付方式

四、履约保证金

五、验收标准和方法

六、甲方的权利和义务

1.甲方有权对合同规定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分XXX。

2.根据本合同规定，按时向乙方支付应付服务费用。

3.国家法律、法规所规定由甲方承担的其它责任。

……

七、乙方的权利和义务

1.根据本合同的约定向甲方收取相关服务费用。

2.接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。

3.国家法律、法规所规定由乙方承担的其它责任。

……

八、违约责任

1.若甲方未按照合同约定逾期向乙方支付货物费用，每逾期一天，按应支付金额的X‰作为违约金支付给乙方，直至实际支付之日

2.因甲方原因导致变更、中止或者终止政府采购合同的，应对乙方受到的损失予以赔偿或者补偿。

……

九、不可抗事件处理

1.在合同有效期内，任何一方因战争、洪灾、台风、地震等不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力事件影响期相同。

2.受阻一方应在不可抗力事件发生后尽快用电话通知对方并于事故发生后XX天内将有关部门出具的证明文件等用特快专递或挂号信寄给对方审阅确认。

3.不可抗力事件延续XX天以上，双方应通过友好协商，确定是否继续履行合同

……

十、解决合同纠纷的方式

十一、合同生效及其他

1.合同经双方法定代表人（或主要负责人）或授权委托代理人签字并加盖公章后生效。

2.政府采购合同履行中，甲方需追加与合同标的相同的货物的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。补充协议签订后，报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3.本合同一式3份，自双方签章之日起生效。甲方持有1份，乙方持有1份，同级财政部门备案1份，具有同等法律效力。

甲方：（盖章）　　乙方：(盖章）

法定（授权）代表人：　　法定（授权）代表人：

地 址：　　地 址：

开户银行：　　开户银行：

账号：

签订日期： 年 月 日

账号：

签订日期： 年 月 日