国家税务总局广东省税务局

政府采购服务类信息化项目

合 同 书

采购编号：GPCGD23C500FG221F

合同编号：

项目编号：粤信项[2023]26 号

项目名称：广东税务 2023 年安全运维项目

甲方：国家税务总局广东省税务局
电话：020-37990977
传真：
地址：广州市天河区花城大道 767 号

乙方：联通（广东）产业互联网有限公司
电话：020-22181979
传真：020-22181979
地址：广州市黄埔区（中新广州知识城）亿创街 1 号 406 房之 555

根据 广东税务 2023 年安全运维项目的采购结果，按照《中华人民共和国政府采购法》、《中华人民共和国民法典》的规定，经双方协商，本着平等互利和诚实信用的原则，双方一致同意签订本合同：

一、合同金额

合同金额为（大写）：人民币￥4,798,000.00 元（肆佰柒拾玖万捌仟元整）。税率：6%，其中不含税金额：4,526,415.09 元（肆佰伍拾贰万陆仟肆佰壹拾伍元零玖分）， 税金：271584.91 元（贰拾柒万壹仟伍佰捌拾肆元玖角壹分）

二、服务范围

甲方聘请乙方提供以下服务：

安全设备运维服务、桌面终端安全管理系统运维服务、数字证书和密码服务组件运维服务，态势感知平台运维服务、省局办公互联网上网行为管理运维服务、“双向”安全交互系统运维服务、安全管理平台运维服务及应用系统安全渗透、网络安全管理制度文档更新完善、应用系统网络安全审核、安全基线配置核查、安全检查、主机漏洞扫描等，需要实现 7*24 小时服务，提供最少 13 人年驻场；已过保的安全设备保修服务；重要时期保障；应急响应；安全检查；安全运维日志审计。

主要包括以下内容

1.安全设备运维日常维护。对省局数据中心所有安全设备进行运维服务，对安全设备日常监控、管理。通过预警检测、安全运维服务，对广东省税务局省级数据中心业务应用区、广域网区、横向联网区、办公区的网络安全设备进行日常监控、管理、补丁系统升级，收集网络和安全设备日志信息并对其进行分析，分析异常行为，配置安全策略，拦截网络攻击，提供提出处理或改进的建议、整改方案。包括不限于防火墙、WebIDS、入侵检测系统、漏洞扫描器、蜜罐诱骗系统、全流量分析系统、堡垒机、SSL VPN、防毒墙等，及供应统、漏洞扫描器、蜜罐诱骗系统、全流量分析系统、堡垒机、SSL VPN、防毒墙等，及供应商带的安全设备的运维维护。提供备机备件，保证安全设备的高效稳定运行。在服务期内用户新增的同类网络安全设备也在运维服务范围内。交付方式：现场。交付成果：《安全设备运维方案》《安全设备运维月报》等。

2. 终端安全管理系统运维服务。对全省已建桌面终端安全管理系统进行运维，保障广东税务系统计算机终端稳定运行，对系统进行日常维护、日常运行监测、补丁升级等，对接总局运维服务团队。确保网络准入控制，终端行为管理，身份与安全状态检查，防病毒软件检查，操作系统补丁安装，防止直接访问数据泄露，资产管理与定位，内网违规报警和事件源进行定位等系统全部功能的使用,同时对自建的终端准入管理系统进行运维管理，对国产终端的杀毒及服务器运维管理。交付方式：现场。交付成果：《计算机终端管理系统服务方案》《安全运维月报》等。

3.数字证书运维服务。对数字证书系统进行运维服务，保障数字证书系统稳定运行。

（1）日常运维：对省级注册与发布系统（含内、外部两套）进行现场运行维护，对接总局运维服务团队。负责省级注册发布系统及其配套通用设备、加密设备的运行、维护及数据备份等工作，保证系统的正常运行和服务。负责向省级、市级及区县级制证点相关人员提供技术支持，税务 UKEY 申请初始化系统运维。

（2）加强硬件设备及系统的日常巡检，每天定时检查硬件设备的运行情况，检查系统的运行情况，发现故障及时处理，硬件及系统巡检要求每天至少上午、下午各一次，做好巡检记录。加强注册系统与发布系统的数据备份，每天至少一次数据备份，每次备份数据至少有两处存放保留，并做好备份记录。对于已做自动备份的，运维人员应做好数据备份的检查工作，确保系统数据备份正常。日常巡检发现设备故障，应及时联系设备厂商进行处理，同时上报总局运行维护人员，由总局运行维护人员判断硬件故障对系统的影响，做好相应的应急处置，配合设备厂商解决故障问题，并及时恢复系统正常运行，同时做好记录。日常巡检发现软件系统故障，应及时上报总局系统运行维护人员，由总局系统运行维护人员进行系统检查和故障分析，现场运维人员配合总局系统运行维护人员及时解决故障问题，同时做好记录。对于不能及时解决的非常规软硬件故障，应及时采取应急措施保证系统正常服务。

（3）运维人员应根据每个月的系统运行维护情况汇总整理形成《XX 省税 XX 年 XX 月税务数字证书系统运维月报》。

4.态势感知平台运维服务。对态势感知平台进行运维服务，保障态势感知平台稳定运行。对系统进行日常维护、日常运行监测、补丁升级、资产配置更新等，对接总局项目运维服务团队。1.每天对态势感知平台及相关安全设备进行巡检，以保证设备健康运行，定期配合研发对平台及相关设备进行升级，以确保平台功能和安全策略满足要求。2.每日配合安管运维人员核对取数的准确性、完整性，配合安管运维人员调整态势感知平台安全策略。3、安全监测要求:需开展常态化的日常告警监控工作，定期跟踪事件处置情况，高危安全事件的通告工作等。4、态势感知平台资产管理和发现，对资产进行识别、分类以及标记管理工作，对网络中可能存在的未知资产进行动态识别，对资产进行更新。输出文档要求：《XX 省税 XX 年 XX 月态势感知平台系统运维月报》。

5.省局办公互联网网络行为审计系统运维。对省局已建办公互联网网络行为审计系统运维，保障广东税务省税务局的办公互联网计算机安全合规稳定运行。确保外网网络准入控制，终端行为管理审计，身份与安全状态检查，违规报警和事件源进行定位等系统全部功能的使用，建

立外网计算机清单控制管理。交付方式：现场。交付成果：《办公互联网网络行为审计系统服务方案》《审计月报》等。

6.已过保的安全设备保修服务。已过保的安全设备维保，包括硬件、软件版本及特征库的续保。需续保设备清单详细见招标文件的采购需求。

提供为期一年，证书类型为通配符，证书类型为 DV（域名型）且证书规格为 Digicert 的 SSL 证书，供*.guangdong.chinatax.gov.cn 域名使用。

7.应用安全渗透测试。提供应用安全渗透测试服务，对广东省税务局省级数据中心业务应用区、广域网区、横向联网区、办公区的网络系统、信息设备、数据库、中间件、省级应用系统和网站群、微信、移动 APP 和办税系统进行日常安全扫描和渗透测试，收集信息并对其进行分析，检查网络和系统漏洞，查找设备和系统的不足。分析异常行为，收集入侵行为信息并对其进行分析，配置安全策略，拦截网络攻击，提供整改方案；提供省局互联网出口安全防护服务及全省互联网应用系统漏洞检测服务，结果进行审核确认并提出安全加固意见。提供工具：渗透测试所需工具和软件。交付方式：现场。交付成果：《应用安全扫描和渗透测试方案》《应用安全扫描和渗透测试月报》《互联网应用防护及检测报告》。

8.重要时期保障。做好特殊重大保障时期（包括"两会"、攻防演练、春节、国庆等重要节假日、重大政治、军事活动或社会活动等)的信息安全保障工作和值班，在确保常规的 7*24 值班服务基础上，根据省税务局需要增派人员进行 24 小时值班值守；特殊情况下，增派资深安全专家并协调相关外部资源提供保障和检查，保证在上述关键时间点客户能够得到相比平时更高级别的保障，在攻防演练期间服务供应商应根据现场实际情况，提供专业的安全技术专家与采购人协同防护，全面提升客户的安全应对能力，降低安全事件的发生概率。交付方式：现场，交付成果：《XX 网络安全保障方案》。详细见招标文件的采购需求。

9.应急服务人员响应。除重要时期保障外，在驻场人员无法解决所遇到问题情况下，提供网络安全专家团队开展应急响应，组织安全调研分析，分析现场问题，进行现场取证溯源，完成证据链分析工作，提交分析响应报告。网络安全专家团队提供 7*24 小时支持响应，5 分钟响应，必要时候 1 小时到达现场。

10.密码服务组件系统运维。对密码服务组件系统进行运维服务，保障密码服务组件系统稳定运行。对系统进行日常维护、日常运行监测、补丁升级，业务应用发布配置等，对接总局运维服务团队。1.日常维护，每日早中晚三次定期检查+每日工作时间不定时抽查，检查服务器状态是否正常，查看所有服务显示状态是否正常，关注系统的连通性和可用性，对业务数据进行监控。2.对涉及的硬件设备（包括但不限于：密码机、签名验证服务器等）开展巡检和健康检查。3.在密码组件中对采购人指定的需要对接密码组件服务的应用系统进行对接配置，使用密码组件系统功能对接入的税务应用系统的各项密码服务内容进行配置。4.熟悉安全管理员、安全审计员、

系统管理员等岗位对密码组件系统的操作运维。输出文档要求：《XX 省税 XX 年 XX 月密码组件服务系统运维月报》《周报》。

11.“双向”安全系统运维。对“双向”安全系统进行运维服务，保障“双向”安全系统稳定运行。对系统进行日常维护、日常运行监测、补丁升级，业务应用对接的安全策略配置等，对接总局运维服务团队。1.日常维护，每日早中晚三次定期检查+每日工作时间不定时抽查，检查服务器状态是否正常，查看所有服务显示状态是否正常，关注系统的连通性和可用性，业务监控、节点监控、应用状态。2.对涉及硬件设备的巡检和健康检查。3.为采购人指定的其他与“双向”安全系统对接的应用系统进行对接配置，通过“双向”安全交换系统为这些应用进行安全策略配置，确保应用的安全有效性及配置文档资料的归总。4.加强对“双向”安全交换系统的稳定性监测管理。输出文档要求：《XX 省税 XX 年 XX 月“双向”安全系统运维月报》《周报》。

12.网络安全管理制度文档更新完善。服务商应参照网络安全等级保护 2.0、国家税务总局和广东省税务局有关规定，结合广东税务实际工作情况，修订和完善采购人指定的适用于广东税务的网络安全管理制度文档，保证网络安全管理制度文档既能符合广东税务信息系统建设发展需要，同时又能够满足国家税务总局在网络安全工作方面的要求。

13.应用系统网络安全审核。为服务期内广东省税务局新建的或局方指定的其他需要开展安全“三同步”工作的应用系统提供全生命周期的安全审核相关服务，依据《税务应用系统网络安全审核指南（试行）》、税务总局《网络安全工作责任分工表》等规范，对新建的或局方指定的其他需要开展安全“三同步”工作的应用系统提供规划阶段、设计建设阶段、使用阶段（日常运维阶段）的全生命周期的安全咨询、评测等服务；为已上线系统提供安全评测服务。详细见招标文件的采购需求。

14.安全基线配置核查。对广东省税务局指定的设备开展安全基线配置核查工作，根据核查结果协助广东省税务局优化指定设备的安全配置，包括但不限于帐号管理、文件权限等。详细见招标文件的采购需求。

15.安全检查。在服务期内协助广东省税务局开展各项网络安全检查工作，包括省局自查、外单位对省局的检查等；此外，需要时对指定的地市开展网络安全检查工作，以辅助相关市局落实网络安全检查工作任务，工作过程中根据实际情况提供设备、检测系统、技术或临时增加人员等支持。

16.主机漏洞扫描。需使用业界知名的、成熟的漏洞扫描工具对广东省税务局指定的设备、系统、数据库、中间件等提供主机安全漏洞扫描服务，收集漏洞信息并对其进行分析，形成漏洞扫描报告提交给局方；对于完成整改的，需重新进行漏洞扫描并出具相应的报告。

17.7*24 小时服务-值班。提供运维值班人员，保证 7*24 小时的不间断运维值班服务，法定工作时间保证 10 人在岗，其余时间实行三班倒上班制度。对运维的所有安全设备及系统开展值班监测，及时发现设备是否异常，是否有异常攻击行为，开展实时应急响应处置工作。

18.对安全管理平台运维。对安全管理平台系统运维，熟知安全管理平台技术架构、平台功能和部署情况，能通过安全管理平台熟练处置各类安全事件，对系统进行日常维护、日常安全监测、补丁升级等，对接总局运维服务团队，配合做好总局绩效考核工作。具体内容详细见招标文件的采购需求。

19.其它需要的未列安全服务详见招标文件的采购需求。

三、甲方乙方的权利和义务

1. 甲方的权利和义务

（1）甲方应当为乙方有效完成技术支持服务提供必要的支持，包括提供工作场所、及时下达工作任务，使乙方更好地完成工作任务而协调必要的业务和技术支持；

（2）甲方有权要求撤换不合格的现场服务人员,乙方应及时配合。如撤换超过两次仍未达到甲方要求，甲方有权解除合同，乙方除应在收到解除合同通知书之日起 10 日内退还甲方已支付但未提供服务部分的费用，还应按照合同总价的 20%向甲方支付违约金，并赔偿由此给甲方造成的全部经济损失。

（3）若乙方在接到甲方请求后未按本合同约定或甲方要求的时间进行响应或解决问题的，甲方有权委托第三方进行处理，由此产生的费用由乙方承担。

2. 乙方的权利和义务

（1）乙方组建项目组，配置 1 名有 5 年以上网络安全项目管理经验的项目经理、13 名以上有 2 年或以上网络安全工作经验具备相关证书的驻场工程师，最少 2 人具有 NISP 或 CISP 认证或高级网络安全证书。（其中 2 名具有三年以上网络安全运维工作经验的安全设备运维人员，1 名有 1 年以上的终端安全管理系统管理经验的运维人员、1 名具有 1 年以上的数字证书系统及密码组件服务系统运维经验的运维人员、1 名具有一年以上的态势感知平台运维经验的人员、1 名有三年以上丰富渗透经验的安全渗透人员、1 名具有一年以上双向安全交换系统运维经验的人员、2 名应用安全审核工程师、1 名日志审计工程师、3 名以上的 7*24 小时服务-值班工程师），遵从甲方的管理制度、网络安全管理规定及相关规定。

（2）特殊保障的专家人员、攻防演练时期提供的专家。乙方应当至少提供 2 名安全专家和 2 名高级安全工程师（应根据实际情况进行酌情增派），按需自行配备所需专业工具。1）安全专家需具有注册信息系统安全专家（CISSP）、注册渗透测试专家（CISP-PTS）、信息安全保障人员认证（CISAW）等资质中的 2-3 个，拥有 3 年以上省部级以上安全保障成功防守案例；2）高级安全工程师必须至少具有注册信息安全专业人员（CISP）、注册信息安全工程师（CISE）、注册渗透测试工程师（CISP-PTE）资质中的其中一个。

（3）非工作时间，乙方派遣的驻场工程师及项目经理必须 24 小时开机，随时与甲方保持联系。乙方接到甲方应急响应请求后，需在半小时内作出响应 2 小时内派工程师到达甲方广州

市指定办公地点，4 小时内到达广东南海税务信息处理中心、广东税务五山数据中心。（4）乙方派遣的驻场工程师应当每月 30 日前提交一份安全月报，描述甲方信息安全总体情况，并协助甲方定制安全评价指标体系，提供展示图表；乙方应当每半年提交一份安全服务报告。对重大安全事件，须提交独立报告，详细描述从发现到解决的完整过程。

（5）除甲方已有的安全设备、工具或软件外，乙方应当向甲方免费提供安全服务还需要的其它资料、设备、工具或软件。乙方为执行本合同而使用的网络分析、漏洞扫描、渗透测试等可能影响网络性能的工具应符合公安部门备案要求或经甲方授权后方可使用。

（6）乙方在合同生效后一个月内按采购需求提交书面的完善的服务方案，服务方案须列明服务内容、进度安排以及验收标准。服务方案将作为项目初验及最后验收的标准。

（7）乙方需保证实际驻场人员与投标书相符，服务中途若需更换人员，更换人员应为同等或以上资质（学历、资历等）人员，并提前一周以书面形式征求甲方意见，未经甲方书面同意不得进行调整。

（8）未经甲方书面同意，乙方不得安排驻场人员进行非本项目服务的其他工作。乙方应为其工作人员足额支付工资、购买社保、发放福利补贴等，乙方与其工作人员之间的一切纠纷与甲方无关，因此导致甲方的损失由乙方承担。

（9）乙方必须保证工作质量。在项目实施期间，乙方必须根据项目完成进度及时将服务过程中产生的各类资料（包括服务方案、安全规划、管理制度、安全月报和年报、测评报告、评估报告、检查方案等）交付甲方。

（10）乙方及其驻场人员须与甲方签订网络安全及保密协议，驻场人员须遵循甲方的各项规章制度。所接触的广东税务专有信息仅限于本人在本项目中使用，不得向他人泄露，更不得用于演示或宣传。

（11）乙方为执行本合同而提供的资料、设备、工具或软件不得侵犯第三方的知识产权。如发生知识产权纠纷，由乙方承担相应的责任。

（12）乙方应当通过技术手段，对甲方关键信息系统资产面临的安全隐患和风险及时提出预警、整改建议或风险评估；提供应用安全扫描和渗透测试服务、预警检测、安全运维、网络安全数据分析服务、省局互联网出口安全防护、及全省互联网应用系统漏洞检测服务；提供甲方在特殊时期及新设备接入时的网络安全保障。

（13） 已过保的安全设备维保服务。

四、服务期间（项目完成期限）

1.委托服务期：自合同签订之日起一年（其中，安全管理平台运维服务的服务期为 2024 年 6 月至项目结束），若服务期满但仍存在部分服务未完成，服务结束日期相应顺延，直至所有服务完成。

2.服务地点：甲方广州市指定办公地点、广东省税务五山数据中心、南海数据中心。

五、 付款方式

由甲方按下列程序向乙方指定账户付款：

1.在本项目合同签订并收到等额增值税普通发票后 30 个工作日内向乙方支付合同总额的 50％ ，即人民币￥2,399,000 元（大写：人民币贰佰叁拾玖万玖仟元整）作首期款，合同结束，乙方完成全部服务事项通过验收并开具发票后 30 个工作日内，支付合同余额，即人民币 ￥2,399,000 元（大写：人民币贰佰叁拾玖万玖仟元整）。

2.每笔款项支付前五个工作日内，乙方应向甲方提供与应付款项等额的合法有效的增值税普通发票（含货物款发票、货物安装费发票及有关服务发票）。

3.本合同的付款时间为甲方向政府采购支付部门提出支付申请的时间（不含政府财政支付部门审查的时间），如因政府财政支付管理流程导致的支付延期，甲方不承担逾期付款责任，也不作为乙方迟延履行或不履行合同义务的理由。

六、知识产权归属

1.乙方应保证，甲方在中华人民共和国使用该软件产品（或货物、或系统）或其中任何一部分时，如受第三方提出的侵犯其专利权、商标权或其他知识产权的起诉，乙方承担一切责任。甲方因第三方主张权利造成的损失，无论发生在合同期内、合同期满或解除后，甲方均有权向乙方追偿全部损失（包括但不限于赔偿费用、诉讼费、律师费等）。

2.乙方在执行合同中向甲方提供定制开发服务所产生的所有技术资料、文档和软件系统（包括源代码和可运行系统）的所有权和软件著作权归甲方所有。

3.乙方为执行本合同而提供的第三方技术资料、软件、工具及乙方已有知识产权产品的使用权归甲方所有。

4.乙方在执行本合同的内容定制开发或者主要是利用甲方的物质技术条件所完成的职务发明，甲方享有知识产权，乙方不得未经甲方明确授权的前提下利用这些成果进行生产、经营，亦不得自行向第三方转让或允许第三方使用。

七、保密

1.甲乙双方的保密协议将于合同签署时生效，本协议签订之日起至本协议终止之日后满 5 年。

乙方驻场人员须遵循甲方的各项规章制度，工作时间不得从事任何与工作无关的事情。未经甲方事先书面同意，乙方不得将由甲方为本合同提供的条文、规格、计划、样品或资料提供给与本合同无关的任何第三方，不得将其用于履行本合同之外的其它用途。即使向与履行本合同有关的人员提供，也应注意保密并限于履行合同所必需的范围。

甲方不得将由乙方向甲方提供的产品技术方案、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、实验数据、试验结果、操作手册、技术文档等技术资料，以及甲方所知悉的乙方经营策略、客户名单、采购资料、定价政策、财务资料、进货渠道等商业信息提供给与本合同无关的任何单位或个人。

2.除了合同本身之外，上款所列举的任何物件均是甲方的财产。如果甲方有要求，乙方在完成合同后应将这些物件及全部复制件还给甲方。

3.技术支持过程中（含系统开发过程）至乙方正式向甲方交付文档资料时止，乙方必须采取措施对本项目过程中的数据、源代码、技术文档等资料保密，否则，由于乙方过错导致的上述资料泄密的，乙方必须承担相应法律责任。

4.项目中所涉及的双方的内部资料、数据、业务流程、工作规范和开发过程中产生的文档记录以及其它商业信息，甲、乙双方均有责任承担保密义务。未经对方许可，任何一方不得以任何形式向其他方泄露。

5.乙方保证乙方及其工作人员对在服务过程中所了解、知悉的甲方或相关单位的政府信息不得对外泄露，否则应负全部法律责任。

八、违约责任与赔偿损失

1.乙方违反本合同约定的义务或提供的产品、服务达不到甲方要求的，经甲方通知改正仍不改正或改正仍达不到甲方要求的，则甲方有权解除合同，乙方应向甲方返还已支付但未提供服务部分的款项，并支付本合同总额的 20%作为违约金。

2.乙方未能按本合同规定的时间提供服务，从逾期之日起每日按本合同总价 5‰的数额向甲方支付违约金；逾期 15 天及以上的，甲方有权解除合同，双方按已提供服务的期限及内容结算服务费后，乙方向甲方支付本合同总额 30%的违约金，由此造成的甲方经济损失由乙方承担，包括但不限于甲方委托第三方处理产生的费用等。

3.乙方未按照招标文件、本合同约定的要求提供服务，引发金税三期核心征管系统、外部交换系统、税库银系统、社保费标准版、增值税发票管理系统（含税控和底账）、电子税务局等全省业务系统以及税务数字证书系统（省税务局端）、密码服务组件系统、双向安全交换系统等基础系统出现故障（不可抗力因素除外），导致全省范围内业务中断，持续时间超过 4 小时，乙方须按照合同总价款的 10%向甲方支付违约金，给甲方造成损失的，乙方需承担赔偿责任。若后续事故未能在 24 小时内解决，或者类似事故一个月内发生 2 次以上，甲方有权解除本合同，并且不予支付合同尾款。

4.甲方逾期付款，每日按应付未付款的万分之一向乙方偿付违约金，违约金总额累计不超过合同总金额的 5%。

5.乙方不得另行开发本合同业务需求范围内、供纳税人(或缴费人)使用的软件,如有违反，甲方将乙方纳入税务系统信息化服务商失信名单

6.乙方在本项目实施过程中发生违反网络安全规定行为，造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定之日起三年内，税务系统各单位可以拒绝乙方参与税务系统政府采购活动。

7.乙方应建立防止违法违规聘用离职税务人员的风险控制制度。乙方违法违规聘用离职税务人员的，甲方有权视情况采取以下一项或多项措施：

①甲方要求乙方限期改正；

②乙方按合同总价 10%的数额向甲方支付违约金；

③乙方 3 年内不得参加所聘人员原单位及下属单位的信息化项目政府采购活动；

④甲方有权解除部分或全部合同；

8.乙方需保证所提供服务的正常运作，如出现纳税人投诉或相关部门反馈监督意见等情形的，每出现一次乙方需支付本合同总额 1%违约金，并赔偿甲方遭受的损失。

9.如乙方存在违背保密协议或廉政协议约定义务的行为，甲方有权解除合同，乙方须一次性支付本合同总额 30%的违约金，由此造成的甲方经济损失由乙方承担。

10.乙方因违反本合同约定所需承担的违约金、赔偿金等，甲方有权直接于应付款中予以扣除，如不足以抵扣的乙方须赔偿补足。

11.本合同履行过程中一方违约的，违约方应赔偿守约方的损失，包括但不限于律师费、诉讼/仲裁费、公证费、差旅费、保全费、担保保函费等费用。

12.乙方在合同履行期间存在“围猎”甲方税务人员行为的（指以获取不正当利益为目的，采取馈赠礼品礼金、邀请娱乐旅游消费、提供便利条件等非正常交往手段“围猎”相关税务人员及其亲属），自甲方及甲方主管机关认定或通报之日起三年内，甲方可以拒绝乙方参与其政府采购活动。

13.国家税务总局发票电子化改革（金税四期）领导小组办公室可以对《税务系统信息化服务商失信行为记录名单制度(试行)》制度列举的失信行为进行认定，经其认定存在失信行为的服务商，3 年内限制参加税收信息化项目政府采购活动。

14.其它违约责任按《中华人民共和国民法典》处理。

九、争议的解决

1.合同执行过程中发生的任何争议，如双方不能通过友好协商解决，任一方可向甲方所在地有管辖权的人民法院提起诉讼，按相关法律法规处理。

十、不可抗力

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后 1 日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或对方谅解确认后，允许延期履行或经对方同意修订合同，并根据情况可免于承担部分或全部违约责任。

十一、税费

与本合同相关的税费，依中国的税法规定由相应的承担方承担，本合同总价为含税价。

十二、其它

1.本合同所有附件、招标文件、投标文件、中标通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2.在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议）即成为本合同的有效组成部分。

3.如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4.除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。如乙方擅自部分或全部转让其应履行的合同项下的义务的，甲方有权解除合同，双方按已提供服务的期限及内容结算服务费后，乙方向甲方支付本合同总额 20%的违约金，由此造成的甲方经济损失由乙方承担，且甲方有权根据国家税务总局相关规定将乙方列入信息化服务商失信行为记录名单。

十三、合同生效

1. 本合同在甲乙双方法人代表或其授权代表签字盖章后生效。

2. 合同一式陆份，甲方执肆份，乙方执贰份，具有同等的法律效力。

3. 附件：

附件 1：项目需求书 （简化版）

附件 2：保密协议书

附件 3：廉政协议书

附件 4：网络和数据安全责任协议书

附件 5：采购评审结果通知

附件 6：乙方项目组核心成员列表

附件 7：报价明细表

甲方（盖章）：国家税务总局广东省税务局

代表（签字）：

日期：

乙方（盖章）：联通（广东）产业互联网有限公司

代表（签字）：

开户名称：联通（广东）产业互联网有限公司

银行帐号：3602 0081 0920 0757 332

开户行：中国工商银行广州高新技术开发区支行

日期：