附件 1

广州市科技项目评审中心信息系统运行维护服务采购需求

第一章 响应须知

最高限价：人民币 34.8 万元。		
资格要求：		
1	符合《中华人民共和国政府采购法》第二十二条的规定。	
2	必须具有独立承担民事责任能力，并在中华人民共和国境内注册的法人。	
3	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采购活动（以国家企业信用信息公示系统 www.gsxt.gov.cn 查询结果为准）。	
4	为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	
5	在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）相关主体信用记录中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。	
是否接受联合体报名：（ ）是（√）否		
采购范围		
1	采购内容	确定 1 家供应商，为采购人提供信息系统运维服务。
2	政策要求	1. 供应商应按照《中华人民共和国劳动法》的相关规定发放工资，服务人员工资不得低于广州市企业职工最低工资标准（工资不含按国家规定供应商必须支付的社会保险及其他应付费用）。 2. 供应商应按照《中华人民共和国社会保险法》和《住房公积金管理条例》的相关规定，支付国家规定必须购买的社会保险费用（基本养老保险、基本医疗保险、工伤保险、失业保险、生育保险）和缴存住房公积金。
3	服务期	总服务期 12 个月。

第二章 项目概况

一、采购人简介

广州市科技项目评审中心为市科技局管理的正处级公益一类事业单位，现有近 30 名工作人员，主要负责科技项目的受理、立项、检查、验收等全过程管理与评审工作，及科技计划项目库、专家库等的建设与管理工作。中心每年组织近千余个科技项目、数百场次的评审会议，共有 5 个信息化会议室，需为评审会议提供人员管理、信息提示、多媒体、录音录像等技术支撑。

二、运维范围

本项目涉及基础设施维护和信息安全维护等方面，全面覆盖了采购人的运行维护需求。

序号	服务内容	维护内容
1	基础设施维护	➢ 桌面信息系统设备维护 ➢ 网络和信息安全设备维护 ➢ 服务器及存储设备维护
2	信息安全服务	➢ 漏洞扫描服务 ➢ 安全加固服务 ➢ 安全巡检服务 ➢ 应急响应服务 ➢ 安全检查服务 ➢ 应急演练服务
3	通信链路采购与维护	➢ VPN 专线租赁
4	驻场运维	➢ 驻场运维人员服务 ➢ 二线技术团队支撑

三、运维模式

本项目运维模式采取外包模式，在采购人的统一规划和指导下，由运维服务供应商负责具体的运维服务工作。

四、运维目标

确保采购人信息系统的硬件系统、系统软件、应用业务系统安全、可靠、稳定运行。做好信息系统维护工作，延长系统使用寿命，加强预防性维护，及时解决信息系统故障，将故障影响程度降低到最小，保证采购人各项工作的正常、有序、顺利的开展。

五、总体要求

（一）本项目对安全性、保密性及规范性要求较高，要求提供高标准、高质量、高效率的服务。

（二）供应商负责制订服务方案，各项规章制度和运维服务年度计划，确定组织架构及人员录用等，项目在实施前要向采购人报告备案。

（三）采购人对项目经理、驻场一线运维人员的设置、录用与管理具有建议权。

（四）根据项目周期和支付节点，供应商应及时提供《项目实施方案》《阶段报告》《项目验收报告》。

（五）在处理特殊事件和紧急、突发事故时，采购人对供应商人员具有指挥权。

（六）供应商对所录用人员要严格审查，保证录用人员无劳动教养和刑事犯罪记录、有上岗资格证。供应商要依法纳税，按照法律法规为录用人员办理用工手续。

（七）供应商各类管理、服务人员按岗位要求统一着装，注意仪容仪表及言行规范。

（八）供应商在做好服务工作的同时，有责任向采购人

提出合理化建议，以提高管理效率和服务质量。

（九）具备服务应急预案，具备利用自身资源满足临时应急抽调含系统工程师、软件工程师、网络工程师、网络安全工程、桌面运维人员等专业人员一次性不少于 10 人的调遣能力，以及安排相关设备的使用。

第三章 运维需求

一、基础设施运维

（一）设备清单

序号	设备名称	品牌型号	数量	备注
1	台式及便携式计算机	Lenovo/DELL/HP	40	日常办公用途
2	复印机、传真机、打印机和扫描仪	惠普、震旦等	10	
3	投影仪	日立	1	
4	其他	合同期内新增的系统及设施		

（二）服务内容

1. 配合采购人做好信息化资产管理工作。

2. 做好桌面系统硬件故障（台式电脑、笔记本电脑及其他相关外设）的排查和处理，及时排查原因、修复故障；如遇硬件故障，应及时进行维修或更换，保证设备尽快恢复使用。

3. 协助开展桌面系统（包括电脑、打印机、扫描仪等）的搬移、安装与调试工作。

4. 协助做好操作系统、办公软件的安装、卸载及故障排

查。

5. 维护网络环境，配置网络权限，做好电话、网络线路及终端维护及其他网络技术支撑工作。

6. 及时提醒更换桌面系统耗材。

7. 协助采购人进行设备维修管理。

8. 协助做好桌面系统的病毒防护工作。

9. 做好维护工作的记录及问题梳理，形成知识库，适时开展桌面系统使用技巧及常见问题的培训。

10. 其他交办的基础设施运维服务工作。

（三）服务要求

5×8小时驻场支持、5×24小时热线支持、二线应急支持。

在接到服务需求后，须在5分钟内响应，10分钟内到达现场，及时处理；如果因硬件问题需要维修或更换，协助采购人进行售后、维修。

（四）服务成果

《维护日志》《信息化资产清点记录》。

二、信息安全服务

（一）漏洞扫描服务

1. 服务范围

各业务应用系统及其服务器、数据库、应用服务。

2. 服务内容

（1）系统漏洞扫描。扫描范围包括管理远程工具、访问控制、系统账号、root远程登录、口令策略、FTP用户账号控制、日志记录、日志存储、日志保存、日志系统配置文

件保护、日志文件保护、服务优化、Umask 权限、控制用户登录会话、关键文件的安全保护等相关配置等。

（2）数据安全审计。对访问数据的连接授权、访问授权、攻击保护、连接监控、审计等管理活动实施安全审计。针对数据库的风险行为和违规操作做出防护与告警。分析当前各类数据库所受的威胁和防火墙的应对防护能力，确保数据安全。

（3）应用安全扫描。利用漏洞扫描软件针对服务器运行的基本应用服务（WEB 、DNS、FTP）进行安全测试，测试内容包括帐户安全、应用脚本等。

（4）其他安全扫描。采购人要求的运维范围内的安全专项检查并出具专项检查报告，相关费用由供应商承担。

3. 服务方式

专项检查以及每季度至少开展 1 次（全年共 4 次）常规漏洞扫描服务，包括但不限于对主机系统、数据库和信息系统安全漏洞扫描，及时排查潜在安全风险，形成安全扫描报告，提出安全加固建议。

4. 服务成果

《漏洞扫描报告》。

（二）安全加固服务

1. 服务范围

各业务应用系统及其服务器、网络设备、信息安全设备。

2. 服务内容

（1）服务器安全加固服务

根据漏洞扫描结果，开展以下服务:

A. 分析主机系统的任务和服务类型;

B. 检查分析现有系统的安全漏洞和黑客后门等;

C. 安装最新的服务包（Service Pack）;

D. 选择安装适当的安全漏洞补丁（Hotfix 等）;

E. 关闭系统缺省打开的不必要服务;

F. 删除系统缺省设置的、以及其它原因设置的不必要帐号;

G. 安全配置操作系统注册表参数;

H. 安全配置文件属性;

I. 安全配置系统缺省日志体系;

J. 配置访问控制策略;

K. 其它。

（2）数据库系统安全加固

根据漏洞扫描结果，数据库系统的修补、加固和优化主要有以下内容:

A. 安装补丁（Patch）;

B. 升级或更换程序;

C. 去除后门程序;

D. 修改配置和权限;

E. 制定专门的解决方案。

（3）关键网络设备加固

A. 优化安全策略并实施;

B. 根据策略对设备进行检查与设置，并进行优化调整。

（4）安全设备加固

A. 优化安全策略并实施;

B. 分析设备日志，排查网络的安全隐患及问题;

C. 根据策略对设备进行检查与设置，并进行优化调整。

（5）其他加固。根据采购人专项加固要求，进行专业分析、制定加固方案并进行加固，软件或服务类相关加固费用由供应商承担。

3. 服务方式

专项加固以及每季度根据漏洞扫描开展 1 次（全年共 4 次）常规安全加固服务，加强安全风险防御能力。

4. 服务成果

《安全加固报告》。

（三）安全巡检服务

1. 服务范围

各业务应用系统及其服务器、存储设备、网络设备、信息安全设备。

2. 服务内容

（1）对各业务应用系统及其服务器、存储设备、网络设备、信息安全设备状态、响应时间、下载速度、HTML 加载时间、敏感字、关键内容、攻击、挂马、漏洞等进行检查。

（2）定期对服务器、安全设备、网络设备、应用系统进行专业检查和日志分析，真对系统警告、异常情况、错误信息等进行分析，提供相关分析报告，排查可能存在的隐患，做到事前预防;

（3）根据分析结果提出对安全策略、软件系统、设备设施等方面的优化建议，对相关软硬件系统设施进行加固并协助采购人整改到位;

（4）开展定期的技术交流。

3. 服务方式

每季度开展 1 次（全年共 4 次）常规安全巡查服务。另外，根据采购人专项巡检要求，进行专项巡查，明确巡查要点，开展技术分析，出具专项巡查报告，相关费用由供应商承担。

4. 服务成果

《巡检报告》。

（四）应急响应服务

1. 服务范围

提供不少于 2 次政务外网和办公内网内发生的安全事件应急处置工作。

2. 服务内容

需要处理的紧急安全事件包括:

（1）业务中断;

（2）大规模病毒爆发;

（3）网络瘫痪;

（4）主机或网络异常事件;

（5）数据丢失。

应急响应服务主要包括以下内容:

（1）排查故障，隔离关键数据;

（2）攻击手段分析，提供应急方案或工具软件;

（3）定位攻击来源，提出安全建议;

（4）数据及网络业务恢复。

3. 服务方式

为采购人的突发安全事件提供 7×24 小时的电话技术支持，以及远程响应和现场服务。在处理紧急事件时，通常先尝试通过远程接入的方式定位并解决问题，如果条件不允许或不能解决问题，将尽可能快的赶赴事件现场进行处理，30 分钟内响应，2 小时内到达现场。

4. 服务成果

《应急响应服务确认书》《事故分析处理报告》。

（五）安全检查服务

1. 服务范围

政务外网和办公内网内的日常办公计算机。

2. 服务内容

（1）正版化检查，检查内容主要为日常办公电脑中不能存在未购买或未授权使用的软件;

（2）涉密检查工作主要为日常办公电脑文档信息进行敏感扫描。

3. 服务方式

每年度 4 次现场安全检查服务，包括但不限于正版化检查、涉密检查。

4. 服务成果

《正版化检查检查报告》《涉密检查报告》。

（六）应急演练服务

1. 服务范围

核心网络设备、信息安全设备以及业务系统。

2. 服务内容

全面提高应对突发事件的综合指挥水平和应急处置能力，最大程度的减轻突发事件引起的 IT 系统损失，保障安全事件发生时进行快速响应，保障采购人各信息系统的持续运行。

3. 服务方式

进行 1 次现场演练，包括风险分析、演练组织和准备、演练脚本制作、组织演练及评估、应急预案改进和应急管理工作改进等工作内容。

4. 服务成果

《应急演练方案》《应急演练报告》。

三、通讯链路采购与维护

租赁 VPN 链路，满足移动端访问电子政务外网的需求。专用链路要求：100M 带宽，支持 50 端并发，支持手机、平板、笔记本电脑，支持 IOS、Android、Windows 等系统，并提供相关服务，租赁期一年。

四、运维团队

（一）人员配置及职责

1. 人员配置

运维团队含项目经理 1 名、驻场运维技术人员 1 名、二线支撑团队。本项目中包括服务管理、设备维护、网络管理、

安全管理等内容，需要的服务人员包括如下几类：IT 服务管理专家、IT 设备维护工程师、高级网络工程师、信息安全咨询专家等。系统的维护、故障排除及维修服务，应由具有相应专业资质的（或同等资质）工程师完成。

2. 人员职责

（1）项目经理:

项目经理是项目的管理者，对项目的整体工作负责；组织项目各阶段任务的实施，指导项目组成员工作，确保项目组成员能够履行各自职责，对项目阶段任务的完成情况和质量负责；审查项目管理计划、项目进度报告和项目进展情况；充分熟悉并确认采购人需求，对项目的考核结果是否达到合同要求负责；对维护工作进行紧密跟踪和管理，为项目组调配人力资源和其他资源；与采购人就重大问题进行研讨协调，定时参加采购人组织的项目会议；控制项目的风险，确保项目高效执行。

（2）驻场运维技术人员:

A. 对基础硬件设施以及软件应用系统进行维护;

B. 协助采购人维护、维修有问题的硬件设施;

C. 协助采购人处理在使用软件系统时出现的操作异常、软件基本操作，以及相关的后台数据处理;

D. 在评审业务高峰期，为评审会场提供会议技术保障，确保各项评审工作顺利进行，包括对视频会议系统的设置，视频及音频的调整和维护等;

E. 定期对包括桌面及终端设备、存储设备和机房设备、

网络及信息安全设备等设备进行巡检、维护和清洁工作;

F. 负责协调、联系信息系统运维工作相关各方，跟进问题解决情况;

G. 协助开展网络安全、信息安全等软硬件安全检查工作;

H. 收集、总结日常运维中发现的问题并形成文字材料，积累知识库。

（3）二线支撑团队:

接受一线的服务支持请求，及时与采购人联系，对事件进行调查、记录、归类、分析与支撑；对采购人运维事件进行电话支持，电话中不能解决的，需在约定时间内到达采购人现场，为采购人提供专业服务；事件终止后提供事件的有效处理记录，提高一线处理问题的技能。

（二）人员要求

1. 资质要求:

项目经理（提供资质证明材料及该项目经理在本项目响应截止日之前在本单位任职至少三个月的《投保单》或《社会保险参保人员证明》或单位代缴个人所得税税单等的扫描件）: 具备计算机、通信或电子信息相关专业本科或以上学历；5 年及以上信息系统运维工作经验（提供公司证明）；具有 5 个及以上信息系统运维项目项目管理或实施经验（提供公司证明）；具备有效的 PMP 项目管理专业人员认证证书；具备有效的 ITSS 服务项目经理专业认证证书。

技术团队（提供证书扫描件及在本项目响应截止日之前

在本单位任职至少三个月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等的扫描件）：具有有效的 PMP 项目管理专业人员认证证书；具有有效的 ITSS 服务项目经理专业认证证书；具有有效的信息安全保障人员认证证书（含安全集成、安全运维、应急服务三个注册方向）；其他符合本项目运维内容的专业证书。

2. 能力要求：

人员		能力要求	服务时限	要求
项目经理	项目经理	五年及以上相关工作经验，至少五个同类项目实施及管理经验	工作日 5×8 小时	本科以上
一线运维技术人员	普通工程师	二年及以上专业工作经验，至少一个同类项目实施经验	工作日 5×8 小时	专科以上
二线支撑团队	高级工程师	五年及以上专业工作经验，至少五个同类项目实施及管理经验	7×24 小时故障受理电话服务	本科以上
	中级工程师	三年及以上专业工作经验，至少三个同类项目实施及管理经验		本科以上
	普通工程师	二年及以上专业工作经验，至少一个同类项目实施经验		专科以上

3. 响应时间

（1）工作日服务响应级别

事件级别	一级	二级	三级
故障响应时间	5 分钟	10 分钟	15 分钟
人员到场时间	1 小时	2 小时	4 小时
故障恢复时间	2 小时	4 小时	6 小时
人工技能标准	高级工程师	中级工程师	普通工程师
故障受理方式	手机、固定电话、邮件、QQ、MSN 实时沟通工具等		

（2）工作日以外服务响应级别

事件级别	一级	二级	三级
故障响应时间	5 分钟	10 分钟	15 分钟

事件级别	一级	二级	三级
人员到场时间	2 小时	4 小时	6 小时
故障恢复时间	4 小时	8 小时	12 小时
人工技能标准	高级工程师	中级工程师	普通工程师
故障受理方式	手机、固定电话、邮件、QQ、微信实时沟通工具等		

五、服务成果产出清单

序号	运维内容		服务成果
1	总体要求		《项目实施方案》《阶段报告》《项目验收报告》
2	基础运维		《维护日志》《信息化资产清点记录》《关联性配置》《网络拓扑图》《安全设备部署图》
3	信息安全服务	漏洞扫描服务	《漏洞扫描报告》
		安全加固服务	《安全加固方案》
		安全巡检服务	《巡检报告》
		应急响应服务	《应急响应服务确认书》《事故分析处理报告》
		安全检查服务	《正版化检查检查报告》《涉密检查报告》
		应急演练服务	《应急演练方案》《应急演练报告》
4	通讯链路采购与维护		VPN 专用链路合同

第四章 供应商责任

一、鉴于采购人作为广州市科技项目相关业务对外窗口单位，对内部安全、保密等相关要求较高，因此采购人的信息系统运维管理与一般的运维有较大的区别，在界定责任义务时按有利于采购人的原则执行。

二、在管理服务期内由于供应商责任造成群众、采购人工作人员人身伤亡和财产损失的，由供应商承担全部责任并负责赔偿。

三、供应商的工作人员在辖区范围内发生违法、违规行为的，所造成一切后果及损失由供应商承担全部责任并负责

赔偿。

四、负责承担和支付所属员工的工资福利，依法承担和缴交所属员工的社会保障及规定的税费等费用。

五、合同期满之日，按时撤离，并做好信息系统运维管理服务事项交接和相关资料移交工作。

六、未经采购人书面同意，供应商不得将本信息系统运维管理服务转让给第三方。