附件 1

# 2026 年江海区政务信息化系统商用密码改造项目需求书

## 一、项目名称

2026 年江海区政务信息化系统商用密码改造项目

## 二、项目业主情况

单位：江门市江海区政务服务和数据管理局

地址：江门市江海区金瓯路 288 号

联系人：李耀民

联系电话：0750-3861245

## 三、项目目标

（1）总体目标

按照数字政府建设总体规划和本单位政务信息化规划，结合江海区政务应用系统的密码应用现状与合规需求，通过部署合规可信的商用密码产品，构建全方位、多层次、规范化的密码安全防护体系，确保江海区政务应用系统全面满足《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）的合规指标要求，顺利通过商用密码应用安全性评估（密评）。

（2）本期目标

本期项目重点完成以下建设目标：

1. 密码基础设施完善：在江海区电子政务机房部署密评一体机、综合安全网关等核心密码设备，构建本地化、自主可控的密码运算与密钥管理基础设施；

2. 网络和通信安全加固：通过综合安全网关建立国密SSL加密传输通道，实现政务外网终端访问的传输机密性、完整性保护与身份可信鉴别；

3. 数据安全保护升级：利用密评一体机提供的数据库加解密、文件加解密、完整性校验等能力，对四个政务应用系统的重要业务数据、敏感个人信息、鉴别数据、日志数据实施存储机密性与完整性保护；

4. 身份鉴别体系强化：为系统管理员和运维人员配备智能密码钥匙（USBKey），采用SM2数字证书实现强身份鉴别，替代传统的账号口令认证方式；

5. 物理环境安全提升：更换机房非国密门禁系统为国密门禁系统，配套国密CPU卡和读卡器，落实机房物理出入口的国密算法管控；

6. 管理制度体系健全：建立完善的密码安全管理制度、密钥全生命周期管理规程、人员岗位责任制度及应急处置预案，形成技术与制度并重的密码安全管理闭环。

（3）预期成效

项目建成后，将实现以下成效：

江海区电子政务机房及四个核心业务系统（江门高新区

（江海区）办公自动化系统、江门高新区（江海区）无纸化会议系统、江海区AI智慧政务服务系统、江海区惠企服务平台）全面满足GB/T 39786-2021密码应用合规要求；

政务数据传输和存储的机密性、完整性得到有效保障，敏感信息泄露风险大幅降低；

系统身份鉴别强度显著提升，账号冒用、非法登录等安全事件得到有效遏制；

密码安全管理实现制度化、规范化、流程化，安全事件应急响应能力显著增强；

为江海区数字政府建设的持续健康发展提供安全可信的基础支撑。

**四、项目采购内容**

（一）项目内容

1.专业基础设施服务

采购并部署密评一体机1台、综合安全网关1台、国密门禁控制器1台、国密读卡器1台、卡片录入仪1台及配套国密CPU卡，构建本地化密码运算、密钥管理、安全传输和物理准入管控能力。所有密码硬件须具备商用密码产品认证证书，包含三年硬件保修及系统软件维保服务。

2.配套密码产品服务

采购国密安全浏览器授权40点、单域名 DV 国密SSL证书4个（按四个系统配置）、个人CA证书及USBKey 20套（按四个系统各5套配置），全部授权服务期限为三年，

为终端用户访问、系统通信加密和人员身份鉴别提供配套支撑。

3.业务系统对接改造服务

完成密评一体机与四个政务应用系统（江门高新区（江海区）办公自动化系统、江门高新区（江海区）无纸化会议系统、江海区 AI 智慧政务服务系统、江海区惠企服务平台）的数据库加密对接、签名验签接口集成，完成综合安全网关与业务系统的 SSL 加密传输、访问控制策略配置，完成国密门禁系统与机房现有安防系统的整合部署。

4.密码安全管理体系建设

编制密码安全管理制度、密钥管理策略、人员岗位责任制度、安全操作规程和应急处置预案，组织密码应用安全性评估，确保合规达标。

5.测试、配合密评与验收服务

供应商须完成全部密码设备及系统对接的功能测试、性能压力测试，输出内部测试报告并对测试发现问题落实整改。本项目密评须委托列入国家密码管理局商用密码检测机构目录、取得商用密码检测资质的机构实施（依据《商用密码管理条例（2023 修订）》第十三条、《商用密码检测机构管理办法》第三条）。供应商须全程配合密评机构开展密评测评工作；针对密评机构出具的问题清单，供应商须制定整改方案、逐项落实技术、管理制度问题闭环整改，完成复测直

至取得符合 GB/T39786-2021 要求的合格测评结论，形成完整整改闭环记录文档，同时整理全套项目竣工文档，配合业主完成项目整体验收。

（二）建设要求

**1. 专业基础设施服务**

本项目采购的专业基础设施服务为商用密码产品设备及配套软件授权，具体建设内容如下：

（1）密评一体机

采购密评一体机 1 台，作为本项目密码应用的核心支撑设备，统一承担全系统密钥全生命周期管理、证书管理与密码计算服务。主要功能包括：

密码管理平台：提供密码服务的统一管理和调度能力；

密钥管理：实现密钥的产生、存储、分发、使用、更新、归档、备份、恢复、销毁等全生命周期安全管理；

数字证书管理系统：提供数字证书的签发、更新、吊销、查询等管理功能；

身份认证：提供基于 SM2 数字证书的身份鉴别服务；

数据库加解密：提供数据库透明加密、JDBC 驱动代理加密等能力，支持 SM4 算法对结构化数据进行加密和完整性保护；

电子签章：提供国密电子签章和验章服务。

硬件规格：采用国产化架构设计，包括国产化 CPU 芯片

（具备商密产品认证证书）和国产化操作系统，标准机架式设备；≥32G 内存；≥1TB 硬盘；冗余电源；≥2 个千兆电口，≥2 个万兆光口，三年硬件保修和系统软件维保服务。

性能指标：数据加密插入数据库≥29,000 条/秒，数据密文解密查询≥32,000 条/秒，每秒国密签章≥500，每秒国密验签≥600。

算法要求：对称算法支持国密 SM1/SM4 算法，摘要算法支持国密 SM3，非对称算法支持国密 SM2 算法。

密钥管理要求：采用多级密钥体系，逐层保护，密钥产生，一体机支持产生高质量的随机密钥，密钥存储：支持 256 对 SM2 密钥，任何时候密钥不以明文形式出现在一体机外，密钥的安全使用，密钥由其属性决定使用的许可范围和算法，密钥备份恢复，一体机支持内部密钥的安全备份和恢复，可用于实现互备或负载的多台设备间的密钥同步。

用户与权限管理要求：登录模式支持 UKEY 认证、普通账号密码登录双模式，满足不同安全场景需求。权限分级，支持系统管理员、安全管理员、安全审计员三权分离，权限划分清晰无重叠。用户生命周期管理，支持用户添加、编辑、密码重置、UKEY 绑定/解绑、PIN 码修改等全流程操作。多租户管理，支持多租户隔离，可自定义租户名称、编号，租户间数据独立存储，支持租户资源灵活分配。

密码服务核心能力要求：服务类型支持涵盖电子签章服务、教育身份认证服务、数字证书认证服务、数据库加密服务等，支持服务类型扩展。部署模式支持单实例/多实例部署，

支持集群化部署。提供服务启动、停用、重启、编辑、监控、版本更新、关联应用绑定/解绑等操作功能。资源弹性扩展支持租户自主申请CPU、内存等资源，平台支持审核与配置调整。

资源与集群管理要求：一体机管理支持一体机添加、编辑、删除、详情查看，可关联虚拟机数量统计，支持多区域部署。集群管理支持集群添加、编辑、删除，集群接入点采用HTTPS加密传输，保障集群通信安全。资源分配支持按租户分配CPU、内存资源包，总资源可视化统计，分配比例可调。

扩展性要求：支持新增密码服务类型（如时间戳服务、签名验签服务、动态令牌服务、协同签名服务等），无需修改核心架构。提供标准SDF接口，支持与第三方业务系统对接，实现密码服务调用与数据同步。支持新增一体机、集群节点，扩展过程不影响现有服务运行。服务器资源满足情况下支持租户数量无上限扩展，单个租户可分配资源弹性调整，满足大规模部署需求。

（2）综合安全网关

采购综合安全网关1台，作为系统统一访问入口和安全传输通道的核心设备。主要功能包括：

国密SSL：支持国密SSLv1.1，单端口实现RSA、SM2算法自适应，为B/S架构业务系统提供国密HTTPS安全访问能力；

负载均衡：支持四层、七层负载均衡，多种调度算法和

健康检查机制；

访问控制：支持基于用户、群组、角色、数字证书的细粒度访问控制，支持单点登录和CRL吊销列表拦截；

证书管理：兼容国密、国际标准X.509数字证书，内置国密CA管理中心，可自主签发数字证书。

硬件规格：采用国产化架构设计，包括国产化CPU芯片和国产化操作系统，标准机架式设备，含国密认证密码卡，配置≥6个千兆电口，冗余双电源，三年硬件保修和系统软件维保服务。

性能指标：每秒新建连接数（国密）≥8000，每秒事务数（国密）≥20000，并发SSL连接数≥50000，SSL加密吞吐（国密）≥1Gbps。

国密SSL协议：支持国密SSLv1.1、国际SSLv3/TLS1.0/1.1/1.2/1.3，兼容TLCP协议（GB/T 38636-2020），支持国密双证书双向HTTPS交付，单端口实现RSA、SM2算法自适应，支持TCP、UDP/DTLS协议交付加速，适配FTP、SSH、SIP、物联网等业务，支持国密SSL MQTT协议，配套提供国密MQTT客户端，支持正向SSL代理、RSA与国密SSL协议互相转换，兼容跨域Web资源及301/302跳转，支持X-PID解析与分流转发，支持多类SSL加密套件组合，支持证书导入、CRL证书吊销列表加载。

负载均衡服务要求：支持四层、七层负载均衡，具备轮询、IP哈希、最小连接等多种调度算法，支持ICMP、TCP、

UDP、HTTP、HTML 关键字等多维度健康检查，支持自定义检测规则。

证书管理要求：兼容国密、国际标准 X.509 数字证书，支持密钥、证书、PKCS12 文件导入，支持公安部 CA、CFCA、电子政务 CA 及省级 CA 证书、数字信封导入，支持 SM2/SM3/SM4 国密算法，以及 AES、RSA（1024/2048/4096）国际算法，单服务可配置多条证书链，适配多 CA 证书验证，内置国密 CA 管理中心，可自主签发数字证书。

设备管理要求：支持国密浏览器、国密 USBKEY 双向认证登录管理界面，支持多设备配置同步、Web 在线升级，采用国密算法保障日志完整性，支持日志级别自定义。

（3）国密门禁系统

采购单门国密门禁控制器 1 台、国密读卡器 1 台、国密 CPU 卡 5 张、卡片录入仪 1 台，替换原有非国密指纹门禁系统。国密门禁系统主要特性：

门禁控制器采用嵌入式 Linux 系统，本地支持 10 万人存储容量、60 万条事件记录；

支持刷卡、指纹、密码等多种认证方式及组合认证；

国密读卡器内置国密 SE 安全加密芯片，支持 SM1/SM2/SM3/SM4 加密处理，满足 GM/T 0028 密码模块安全技术要求第二级要求；

国密 CPU 卡支持 SM1、SM4 算法加密，容量 80K byte；

具备防拆报警、消防联动、蓄电池备份、断网续传等功能。

（4）配套密码软件授权

国密安全浏览器：40 点授权，支持 SM2/SM3/SM4 国密算法，具备商用密码产品认证证书，为终端设备提供国密 HTTPS 安全浏览能力；

国密 SSL 证书：4 个单域名 DV 国密 SSL 证书，三年授权服务，按四个系统分别配置，用于综合安全网关国密 SSL 通信；

个人 CA 证书+USBKey：20 套，三年授权服务，按四个系统各 5 套配置,用于系统管理员和运维人员的强身份鉴别。USBKey 装载符合 GM/T 0027 标准个人身份 SM2 数字证书，支持 SM2 签名验签。

（5）密码安全管理体系建设

根据《信息安全技术 信息系统密码应用基本要求》中管理方面的要求，制定与本系统相适应的密码安全管理制度和操作规范，内容至少包含密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置等制度。

1）密钥管理制度

本项目所用密码设备均为通过商用密码检测认证的合规产品，整体密码模块满足 GM/T 0028 安全二级及以上要求，随机数生成符合 GM/T 0005 规范，依托硬件密码模块实现安全密钥生成。本项目不部署独立服务器密码机，整体密码运算、密钥生成由密评一体机承载，设备搭载商用密码服务平台,底层采用具备商用密码认证资质的国密 CPU 硬件密码模块，所有密钥均在密评一体机硬件密码模块内部随机

生成，除公钥外，所有密钥密文均不离开硬件密码模块，全程无明文出模块、无明文落盘。密钥生成过程具备弱密钥检测与剔除能力，保障生成密钥的随机性与安全性。

密评一体机初始化阶段采用门限秘密共享机制生成 3 张管理员密钥卡，实行三人分权保管机制。设备关键管理操作需两名及以上管理员持卡核验登录后方可执行，杜绝单人操作风险。系统落实密钥管理员、密码操作员分权分域管理，密钥管理员负责密钥生命周期管理、操作员账号生成与注销，密码操作员仅负责设备日常配置运维，岗位权限相互隔离、相互制约，有效规避人为操作风险，保障密钥生成环节安全可控。

综合安全网关（国密 SSL 网关）初始化阶段，由设备内置合规密码模块自主生成 SM2 国密算法密钥对,基于设备本地 SM2 公钥完成设备证书申请与签发,实现网关设备通信身份实体鉴别密钥的安全生成。

密钥分发

本项目密钥分发依托密评一体机密码服务平台实现，全程采用密文传输、密钥分离存储机制，所有密钥均不以明文形式对外下发。密钥密文与传输密钥相互独立存储、独立管理，杜绝单次泄露造成整体密钥体系失陷。

本项目支持离线分发与在线分发两种模式，根密钥、密钥加密密钥、信任锚证书等核心根类密钥采用离线介质分发，分发前严格执行操作员身份鉴别；业务会话密钥、临时加密密钥采用在线数字信封+对称加密方式完成安全协商分发，

全程依托硬件密码模块运算保护，保障密钥分发全流程安全合规。

密钥存储

本项目密评一体机、综合安全网关均为通过商用密码产品认证的合规设备，密钥统一存储于设备内置硬件密码模块内部，密钥数据经加密后存储于专用安全存储介质，全程无明文出模块、无明文留存系统内存，所有密码运算均在硬件密码模块内部完成，符合 GM/T 0028 密码模块安全防护要求。

密评一体机采用门限权限管控机制，密钥更新、密钥销毁等高风险操作需超过半数管理员授权同意后方可执行，有效防范人为非法篡改、恶意销毁密钥风险。综合安全网关密钥与设备权限深度绑定，仅授权管理员可执行设备初始化、密钥配置操作，杜绝非法设备接入与恶意配置篡改，全方位保障密钥存储安全。

密钥更新

本项目密钥分为对称密钥与非对称密钥，按照密钥层级与使用场景落实分级更新机制。对称密钥中，一级主密钥、次级主密钥由密评一体机硬件密码模块定期自动更新；业务会话密钥在每次通信会话建立前，通过两端密钥协商机制动态生成、即时更新，保障单次会话密钥唯一性。

非对称密钥方面，管理员、运维人员使用的智能密码钥匙 SM2 公私钥对，通过定期更换、重新申领设备证书的方式完成密钥更新；综合安全网关 SSL 设备 SM2 密钥对，通过

重新生成密钥、向 CA 机构申请新版国密 SSL 证书完成迭代更新，保障非对称密钥长期安全有效。

密钥归档

本项目针对密评一体机内历史业务密钥、弃用加密密钥建立规范的密钥归档管理制度。密钥归档前完成密钥备份文件与备份介质一致性校验，确认可用后纳入归档管理。归档密钥仅用于历史加密数据解密核验，不参与当前业务加密运算。

密钥归档实行“介质分离、双份备份、异地留存”机制，密钥加密文件与密钥备份卡分开存放于不同保密保险柜，同时落实双份存档冗余机制，规避单点丢失风险，全程登记造册、流程可追溯。

综合安全网关 SM2 密钥对主要用于网络通信实体鉴别与密钥协商，不承担历史数据解密校验业务，密钥过期后直接迭代更新，无需开展密钥归档操作。

密钥使用

本项目密钥体系主要包含:综合安全网关 SM2 身份鉴别密钥对、业务数据 SM4 对称加密密钥、数据完整性校验 SM3 密钥。所有密钥均由密评一体机、安全网关内置硬件密码模块物理随机数发生器生成，加密存储于硬件模块内部，全程明文不落地、不外露。

密钥使用前系统自动校验密钥状态与匹配性，规避密钥失效、密钥不匹配导致的业务异常。建立密钥泄露应急机制，一旦发现密钥泄露风险，立即暂停对应业务、紧急更换密钥、

封存泄露密钥，同步上报密码管理主管部门。密钥更新前提前联动业务部门制定切换方案，在硬件密码模块内部完成密钥迭代更新，最大限度保障密钥使用与更新安全。

密钥撤销

当综合安全网关设备证书到期、用户身份变更或密码管理部门提出撤销要求时，由密钥管理员发起密钥撤销申请，经审批后向 CA 机构提交证书撤销请求，完成设备密钥与身份证书的批量撤销与作废，杜绝过期密钥、废弃密钥非法复用风险。

密钥备份

密评一体机具备完善的密钥备份机制，密钥备份操作需满足半数以上管理员联合授权方可执行。备份过程采用门限秘密共享机制拆分密钥备份信息，单次备份使用独立随机加密密钥，实现一次一密，提升备份安全强度。所有备份操作全程登记，记录操作时间、操作人员、设备信息、密钥备份状态，形成完整审计追溯链条。

综合安全网关通信类 SM2 密钥仅用于实时链路鉴别与协商，不涉及历史数据解密，无需备份，密钥过期直接迭代更新即可。

密钥恢复

密评一体机支持合规密钥恢复机制，密钥恢复操作需半数以上管理员授权，通过对应批次的密钥拆分介质即可完成密钥恢复导入，恢复流程全程留痕、登记归档，完整记录操作人员、操作时间、密钥状态，满足三级密评审计追溯要求。

综合安全网关通信密钥无需恢复，密钥失效后直接重新生成新密钥对、更新设备证书即可。

密钥销毁

密评一体机、综合安全网关均具备硬件物理防护能力，具备防撬、防暴力破解、自销毁机制，极端情况下可通过设备初始化完成密钥彻底销毁，杜绝密钥窃取与泄露。日常密钥过期、废弃后，可通过设备合规删除功能完成密钥清零销毁。

本单位建立标准化密钥销毁流程，密钥销毁工作需由建设单位、运维单位、安全管理部门三方人员在场监督执行，销毁完成后三方签字确认，全程台账登记、可审计、可追溯，彻底闭环密钥生命周期管理。

人员管理

本系统严格按照 GB/T 39786-2021、密评三级管理要求完善密码人员管理制度，全面规范密码岗位人员履职、培训、考核与保密管理。

一是建立常态化密码专项培训机制，每半年组织一次密码法律法规、国密标准规范、密码设备操作、密评合规要求培训；项目建成后组织设备厂商开展专项实操培训，确保在岗人员熟练掌握密评一体机、综合安全网关等密码设备的配置、运维与应急操作。

二是落实岗位分权制衡，设置密钥管理员、密码操作员、密码安全审计员三类专职岗位，各岗位均配置 2 名及以上人员，岗位权限相互独立、相互监督、相互制约。其中密码安

全审计员不得兼任密钥管理与密码操作岗位，所有设备账号专人专用，严禁多人共用、混用账号。

三是落实岗前考核与年度继续教育制度，所有密码岗位人员必须岗前培训考核合格后方可上岗，年度密码专项培训不少于4学时，考核结果纳入单位绩效考核。

四是完善密码人员考核、奖惩、保密与调离管理制度，每年开展岗位履职考核，奖惩分明；所有密码岗位人员签订保密协议，明确保密责任，人员调离严格执行离岗审查、权限回收、保密兜底制度。

2）物理环境安全管理制度

严格落实商用密码应用安全性评估三级物理环境安全管理要求，建立完善的机房物理安防管理制度，全方位保障密码设备运行环境安全，筑牢密码体系物理安全底座。机房需部署国密门禁系统，实现机房出入人员身份核验、全程视频留存，严格执行人员出入登记、权限分级管控制度，严禁无关人员进入机房核心区域，杜绝非授权人员接触、操作密评一体机、综合安全网关等关键密码设备。

机房实行7×24小时环境监控与安保值守制度，实时监测机房温湿度、电力、安防状态，保障密码设备长期稳定运行。同时建立密码设备专项物理防护机制，对密评一体机、综合安全网关等核心商用密码设备划定专属部署区域，做好防撞击、防破坏、防水防火、防尘防潮防护，设备具备硬件防撬、防暴力破解、密钥自销毁物理防护能力。严格落实机房设备巡检制度，定期排查物理环境安全隐患，所有巡检、

出入、安防操作全程台账登记、日志留存，做到可追溯、可审计，防范物理破坏、非法接触、设备被盗等风险，保障密码硬件设备及密钥体系的物理安全。

3）建设运行管理制度

严格遵循国标及商用密码标准规范，选用通过国家商用密码检测认证的密评一体机、综合安全网关等合规密码产品，依托密评一体机的国密 CPU 硬件密码模块实现全流程国密运算，不使用无证、不合规密码组件。

密码应用方案编制完成后，委托具备资质的密评机构开展方案评估，评估通过后向单位密码管理部门备案，依据备案方案开展密码应用改造建设。系统改造完成后，全面落实密码应用安全性三级测评，测评通过后方可正式上线运行。系统常态化运行期间，每年开展一次密码应用安全性评估及安全攻防演练，根据测评结果持续整改优化。系统运行期间若发现重大密码安全隐患，立即暂停业务运行，完成整改与复评后恢复上线，保障密码应用体系持续合规、安全有效。

4）应急处置管理制度

成立密码安全应急处置领导小组、应急处置实施小组、应急处置日常运维小组。安全事件发生后，在应急处置领导小组的统一部署下，工作人员各司其职，并严格按照应急处置计划组织实施应急处置工作。

1.应急处置领导小组

应急处置领导小组负责本项目密码安全应急处置的领导和决策，具体职责如下：

负责密码安全应急处置的领导和决策。主要包括制定工作方案，提供人员和物资保证，审核批准应急处置策略，审核批准应急处置计划，批准和监督应急处置计划的执行，开展日常应急演练，指导应急处置实施小组的应急处置工作，启动定期评审、修订应急处置计划以及负责组织的外部协作。应急处置领导小组人员待系统建设完成后确定。

2.应急处置实施小组

应急处置实施小组负责密码安全应急处理的技术保障与具体实施，具体职责如下：

当由于系统崩溃、病毒攻击、非法入侵、软硬件故障等事件发生时，根据密码安全事件的发展态势和实际控制需要，具体负责现场应急处置工作，尽快恢复正常运行。

3.应急处置日常运维小组

应急处置日常运维小组负责做好密码安全的日常巡查及日志保存工作，具体职责如下：

负责做好密码安全的日常巡查及日志保存工作，以保障最早发现异常。同时负责密码安全事件发生后的损失控制和损害评估，并协助应急处置实施小组实施应急处置工作。

应急预案及事件上报

根据《基本要求》中安全管理应急方面的要求，制定密码应用应急策略，并做好应急资源准备，明确密码安全事件处理流程及其他管理措施；针对密码安全方面的应急响应措施包括：当本系统发生密码相关安全事件时，在事发后 3 小时内向我单位密码管理部门进行报告；事件处置完成后 2 个

工作日内，向我单位密码管理部门汇报安全事件发生情况及处置情况。

**五、验收标准**

（一）是否按要求完成合同约定全部服务；

（二）合同约定全部政务信息化系统是否整改完成，通过第三方商用密码应用安全性评估机构测评，取得符合GB/T 39786-2021要求的合格测评结论；

（三）成果文件（设备到货验收文档、设备配置手册、系统对接实施方案、全套密码安全管理制度、培训材料、运维操作手册）是否齐全。

**六、合同履行地点和方式**

合同履行地点为江门市江海区。

**七、报价方式**

（一）公开选取方式为方案择优选取（供应商提供公司简介、报价、资质、技术人员、实施方案等有关情况）。

（二）本项目的报价设置含税最高限价人民币叁拾陆万叁仟肆佰贰拾伍元整（¥363425.00元），包括项目办公设施、食宿、交通、通讯等一切费用，响应报价超过最高限价的，响应无效。

**八、服务时间**

服务期限3个月，自合同签订起算，至项目成果验收合格之日止。

**九、结算方式**

首期款：合同签订后，中选人书面提出支付申请函及与拟支付金额等额的符合采购人财务管理要求的相应发票，确认并启动首期款支付流程。采购人自双方确认进度节点之日起30日内支付，支付金额不高于合同总金额的50%的款项。

尾款：项目终验合格且经采购人确认，中选人书面提出支付申请函及与拟支付金额等额的符合采购人财务管理要求的相应发票后，确认并启动尾款支付流程，采购人自考核验收合格（或双方确认结算/进度）之日起30日内支付，累计支付至合同实际结算金额的100%（含首期款）。部分存在争议不影响其他部分履行的，无争议部分应及时支付。

**十、违约责任**

当事人一方不履行合同义务或者履行合同义务不符合约定的，应当承担继续履行、采取补救措施或者赔偿损失等违约责任。

当事人一方未按照约定支付合同款的，对方可以要求其支付合同款。

当事人可以约定一方违约时应当根据违约情况向对方支付一定数额的违约金，也可以约定因违约产生的损失赔偿额

的计算方法。当事人就迟延履行约定违约金的，违约方支付违约金后，还应当履行债务。

## 十一、补充合同和解决争议方式

采购合同中如有未尽事宜，双方协商一致后可以签订补充合同，但补充合同不得与《中华人民共和国民法典》相抵触。

采购合同履行中需追加服务的，双方可协商签订补充合同，但所有补充合同采购金额合计不得超过原合同采购金额的10%，且不得改变合同其他条款，不得违反《中华人民共和国民法典》合同编的相关规定。

对于合同履行中出现的纠纷，双方应协商解决。协商不成的，可向江门市江海区人民法院起诉。因解决诉讼争议守约方为实现债权支出的合理费用（包括但不限于律师服务费、诉讼费、交通费、保函费、鉴定费、保全费等）由违约方承担。

## 十二、询问、质疑与投诉

（一）询问

响应人对采购活动事项（采购需求书、采购过程和中选结果）有疑问的，可以向采购人提出询问，采购人将及时作出答复，但答复的内容不涉及商业秘密。询问可以口头方式提出，也可以书面方式提出，书面方式包括但不限于信函、电子邮件。联系方式如下：

联系人：李耀民

电话：0750-3861245

邮箱：jhqzsjxxzx@jiangmen.gov.cn

地址：江门市江海区金瓯路288号

邮编：529000

（二）质疑

1.供应商认为采购需求书、采购过程和中选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七个工作日内，以书面原件形式向采购人一次性提出针对同一采购程序环节的质疑，逾期质疑无效。供应商应知其权益受到损害之日是指：

（1）对文件提出质疑的，为获取采购需求书之日或者采购需求书公告期限届满之日；

（2）对采购过程提出质疑的，为各采购程序环节结束之日；

（3）对中选结果提出质疑的，为中选结果公告期限届满之日。

2.质疑函应当包括下列主要内容：

（1）质疑供应商和相关供应商的名称、地址、邮编、联系人及联系电话等；

（2）质疑项目名称及编号、具体明确的质疑事项和与质疑事项相关的请求；

（3）认为采购需求书、采购过程、中选和成交结果使自己的合法权益受到损害的法律依据、事实依据、相关证明材料及证据来源；

（4）提出质疑的日期。

3.质疑函应当署名。质疑供应商为自然人的，应当由本人签字；质疑供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

4.供应商质疑应当有明确的请求和必要的证明材料。质疑内容不得含有虚假、恶意成份。依照谁主张谁举证的原则，提出质疑者必须同时提交相关确凿的证据材料和注明证据的确切来源，证据来源必须合法，采购人有权将质疑函转发质疑事项各关联方，请其作出解释说明。对捏造事实、滥用维权扰乱采购秩序的恶意质疑者，将上报政府采购监督管理部门依法处理。

5.采购人自收到书面质疑之日起7个工作日内作出答复。

6.质疑联系方式如下：

质疑联系人：李耀民

电话：0750-3861245

传真：/

邮箱：jhqzsjxxzx@jiangmen.gov.cn

地址：江门市江海区金瓯路288号

邮编：529000

（三）投诉

质疑人对采购人的质疑答复不满意或在规定时间内未得到答复的，可以在答复期满后15个工作日内，按如下联系方式向本项目监督管理部门提起投诉。

政府采购监督管理机构名称：江海区财政局

地 址：江门市江海区富民路9号

电 话：0750-3831087、0750-3831073

邮 编：529000

传 真：/

**十三、备注**

1.如果监督管理部门对有关服务已经拟定“合同范本”，业主单位、中选服务机构应当使用有关“合同范本”；如果监督管理部门未有“合同范本”，业主单位、中选服务机构应当根据《中华人民共和国民法典》等法律法规的规定自行拟定合同。

2.合同的实质性内容，应当与采购公告、采购结果的内容一致。合同的实质性内容是指合同标的、数量、质量、价款或者报酬、履行期限、履行地点和方式、违约责任和解决争议方法等。

3.合同的变更、终止等，适用《中华人民共和国民法典》等法律法规的规定。

附件：1.合同模板

2.保密承诺协议书

3.廉洁从业承诺书

附件 1

# 合　　同

（此为合同模板，具体以签订合同为准）

项 目 名 称　：　2026 年江海区政务信息化系统商用密码改造项目

委托方（甲方）：

受托方（乙方）：

签 订 地 点　：　广东 省 江门 市 江海 区

# 目　录

第一条　定义

第二条　项目进度计划

第三条　合同价款及支付方式

第四条　甲方提供的条件

第五条　方案认可与验收

第六条　技术支持与服务

第七条　培训

第八条　违约责任

第九条　保密条款

第十条　权利归属条款

第十一条　税收条款

第十二条　不可抗力

第十三条　法律适用和争议解决

第十四条　生效及其他

**附件**

附件一　建设清单

其他附件　/

第一条　定义

1.1　“本工程”或“本项目”：指2026年江海区政务信息化系统商用密码改造项目。

1.2　“系统”：指XXX商用密码应用系统。

1.3　“技术服务”：指对于此系统进行总体规划、设计、安装、调测及保修服务。本合同项下交付内容分为“硬件设备”与“软件系统及技术服务”两部分，其中“硬件设备”指服务器等物理设备（详见附件一），“软件系统”指密码服务管理平台、数字证书认证系统、数据库加解密系统等软件系统及其使用许可（详见附件一）。两部分分别适用不同的增值税税率，具体详见本合同第三条第3.1、3.2款。

1.4　“甲方”:指 _____。

1.5　“乙方”:指_____。

1.6　“双方”：指甲方和乙方。

1.7　“一方”：指甲方或乙方。

1.8　“初步验收”或“初验”：指系统安装、调测、割接、甲方能够正常使用各项功能后，甲方在乙方的协助下对系统进行测试和验证，若达到所有相关技术要求，则双方共同签署相关初验收文件，系统进入试运行。

1.9 “最终验收”或“终验”：指通过试运行期后，甲方在乙方的协助下对系统进行的全面的、最后的检验，以证明其满足技术规范书所有要求。若系统通过最终验收，则双方将签署相关终验合格文件。

1.10 “保修期内技术支持与服务”:指乙方为甲方提供的，自终验证书签发之日起一定时间的保修及技术支持和服务。

第二条 项目进度计划

2.1 乙方应于合同签订后 _____天内，完成本项目设计、实施方案的制定。

2.2 因甲方原因造成乙方不能按期完成工作的，经甲方确认后(确认方式包括：书面、邮件、现场负责人签字等)，乙方工作期可以顺延。顺延的日期与甲方造成乙方不能正常工作的日期相等。

第三条 合同价款及支付方式

3.1 本合同总价（含税价）为人民币大写 XX 整（￥XX 元）。合同价款由以下税目构成：

上述各税目对应金额之和为本合同总价（含税价）。

3.2 发票类型

乙方按国家要求开对应的发票，上述发票载明的各税目金额合计应等于本合同总价（含税价）。

3.3　支付方式：甲方选择以下付款方式（方式二）向乙方指定账户支付合同价款。

3.3.1　方式一：一次性付款

本合同正式签订之日起十个工作日内，甲方应向乙方支付合同总价的100%的款项，人民币大写：/（￥/）。

3.3.2　方式二：分期付款

3.3.2.1　首付款　合同签订后，中选人书面提出支付申请函及与拟支付金额等额的符合采购人财务管理要求的相应发票，确认并启动首期款支付流程。采购人自双方确认进度节点之日起30日内支付，支付金额不高于合同总金额的50%的款项。

3.3.2.2　终验付款　项目终验合格且经采购人确认，中选人书面提出支付申请函及与拟支付金额等额的符合采购人财务管理要求的相应发票后，确认并启动尾款支付流程，采购人自考核验收合格（或双方确认结算/进度）之日起30日内支付，累计支付至合同实际结算金额的100%（含首期款）。部分存在争议不影响其他部分履行的，无争议部分应及时支付。

3.4　乙方的银行信息如下：

开　户 名 称：

开　户　行：

账　　号：

3.5　乙方开户银行、账号等如有变更，应在本合同规定的付款期限前15天，以书面方式通知甲方。

3.6　本项目实施过程中，若甲方中途变更方案或发生设备及其他服务的调整变化以及由此引起的相应费用的变化应经双方另行协商一致后方可执行。

第四条　甲方提供的条件

除本合同其他条款规定的工作外，甲方还负责：

4.1　为乙方的工作提供必备的条件。

4.2　为本合同项下的工程实施提供物质保障。

4.3　向乙方提供本项目所需的各种资料、数据、表格或系统要求。

4.4　指派专人及时参与本项目相关工作。

第五条　方案认可与验收

5.1　系统设计与实施方案的认可

5.1.1　乙方依本合同约定向甲方提交系统设计及实施方案，甲方应当在收到之日起5个工作日内进行评审鉴定及

认可并书面回复乙方，甲方逾期未确认的，视为同意乙方提交的方案。

5.2　验收：甲方选择以下验收方式（方式二）完成本项目验收。

5.2.1　方式一：一次性验收

甲方应在接到乙方关于本项目的验收书面申请之日起10个工作日内指派代表与乙方共同进行验收测试，经测试项目各项设备能正常运行、符合标准的，则由甲方签署乙方提交的验收合格证书。因甲方原因未能按期开展验收工作的，验收期限相应顺延，但不视为项目验收合格。乙方应当予以配合，不得直接要求视同验收通过及支付款项。如测试不满足约定标准，乙方应完成整改后重新提请验收。

5.2.2　方式二：分段验收

5.2.2.1　初步验收

甲方接到乙方关于本项目初步验收书面申请后，应在10个工作日内指派工程技术人员和代表与乙方共同进行初验测试，经测试符合约定的初验测试标准的，则由甲方签署乙方提交的初验合格证书。

由于乙方原因导致初验不合格，乙方应立即进行重新调试，直至测试结果符合约定的初验测试标准；如果重新调试在

15 个工作日后，仍不能达到约定的初验测试标准的，甲方有权终止本合同，并要求乙方返还已经支付的价款。

因甲方原因未能按期开展初验工作的，初验期限相应顺延，但不视为初验合格。乙方应配合甲方后续组织初验，不得以延期为由主张视同初验完毕、要求进入下一阶段或申请付款。

5.2.2.2　试运行和最终验收

初验合格后，系统进入试运行阶段，试运行期为 1 个月。试运行应当符合约定的标准。如果出现不符点，由乙方负责更正和修改，由此产生的费用由乙方承担。同时试运行期间根据更正和修改期间做相应顺延。如果由于乙方原因所引起的应用软件的质量和性能问题造成整个系统瘫痪，并且不能在试运行期内一段合理时间内恢复，试运行期将自系统恢复之次日起重新开始。由于出现上述试运行期的顺延和（或）重新开始导致甲方遭受任何损失或承担任何费用增加，乙方应当赔偿。

因甲方原因造成试运行阶段相关配合工作延误的，试运行期限相应顺延，但不视同试运行完成。

试运行结束后 10 个工作日内进行终验。终验由甲方指派的工程技术人员和代表与乙方共同进行。经终验测试符合约定条件，由甲方签署终验合格证书。终验不合格，由乙

方负责更正和修改，由此产生的费用由乙方承担，并赔偿由此给甲方带来的损失。乙方更正、修改后必须再次进行终验。如果再次终验仍不合格，甲方有权终止本合同，并有权就所遭受的损失向乙方要求赔偿，并要求乙方返还已经支付的价款。

因甲方原因未能按期开展终验工作的，终验期限相应顺延，但不视为终验合格。乙方不得以验收延期为由主张视同终验完毕，不得直接申请支付尾款。

5.3　因甲方要求改变设计方案或其他原因导致工期延误的，经甲方书面确认，工期应按照甲方确认的延误期间作相应顺延。本项目验收标准与方法详见本合同附件一及经甲方书面确认的系统设计与实施方案。

第六条　技术支持与服务

6.1　乙方提供的技术支持和服务（“技术支持和服务”）的内容包括电话支持、现场服务、设备维修支持、电子邮件支持、因特网支持和提供系统应急策略等内容。

6.2　乙方自甲方签署终验合格证书之日起，为甲方免费提供为期 36 个月的技术支持和服务。

6.3　当保修期满后，甲乙双方可另行协商签订技术服务维护协议,以确保系统的正常运行。

6.4　如甲方变更本合同系统使用人、所有人和硬件所有人、持有人，书面通知乙方即可。

第七条　培训

7.1　培训目的

7.1.1　确保甲方技术人员能够熟练地对系统进行运行、诊断、维护和管理；

7.1.2　确保甲方相关业务人员对其使用的应用系统能熟练地操作和使用。

7.2　培训内容

具体培训内容、时间与地点甲乙双方另行商定。

第八条　违约责任

8.1　任何一方不履行或不完全履行本合同约定条款的，构成违约。

8.2　合同一方违反本合同规定，给另一方造成经济损失的，由违约方承担赔偿责任。

8.3　乙方无正当理由造成各阶段工作延期完成，每逾期1日，乙方须向甲方支付本合同总价款万分之二的违约金，如违约金的数额累计达到本合同总价款的10%时，甲方有权终止本合同，由此给甲方造成直接经济损失且上述违约金不足以弥补的，乙方应对不足部分承担损失赔偿责任。

8.4　甲方逾期付款的，每逾期 1 日，甲方须向乙方支付本合同价款总额万分之二的违约金；如违约金的数额累计达到本合同总价款的 1%或逾期超过 30 日的，乙方有权暂停提供服务。如违约金的数额累计达到本合同总价款的 10%或逾期超过 90 日时，乙方有权终止本合同。合同终止后，双方按照合同实际履行情况据实结算，对于乙方已完成且验收合格的工作成果，甲方应当支付对应价款；对于尚未履行部分对应的款项，乙方应当退还给甲方。甲方仍应按约定承担逾期付款违约金，由此给乙方造成直接经济损失且上述违约金不足以弥补的，甲方应对不足部分承担损失赔偿责任。

8.5　有关产品的规格、参数、型号等由甲方提供。如甲方根据乙方提供的生产商和产品资料确定生产商及产品，则有关产品质量由生产商负责。如因产品质量问题造成甲方损失，甲方直接向生产商追偿。

8.6　合规遵循条款

双方应秉承诚实信用原则开展合作，共同遵守法律法规、监管政策、行业惯例及相关合规要求，维护双方合法权益及履行合同可获得之利益。

第九条　保密条款

9.1　保密信息是指：双方之间相互披露的与项目有关的任何信息和数据，包括但不限于任何业务、商业或技术信息和数据，无论这些信息或数据采用何种媒介作为载体，如以有形形式披露、或通过电子通信，包括基于互联网提供。

9.2　双方保证该保密信息仅用于与合作有关的用途或目的。

9.3　双方各自保证对对方所提供的保密信息予以妥善保存。

9.4　双方各自保证对对方所提供的保密信息按本协议约定予以保密，并至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密。

9.5　任何一方在提供保密信息时，如以书面形式提供，应注明“保密”等相关字样；如以口头或可视形式透露，应在透露前告知接受方该等信息为保密信息，并在告知后五日内以书面形式确认，该确认应包含有所透露的信息为保密信息的相关内容。

9.6　双方保证保密信息仅可在各自一方从事该项目研究的负责人和雇员范围内知悉。双方上述人员知悉该保密信息前，该方应向其提示保密信息的保密性和应承担的义务。

经保密信息披露方提出要求，保密信息接收方应按照保密信息披露方的指示将含有保密信息的所有文件或其他资料归还给保密信息的披露方，或者按照保密信息披露方的指示予以销毁。项目终止后，保密信息披露方有权向接收方提出书面要求将保密信息全部载体予以交还。

9.7　上述限制条款不适用于以下情况：

（1）在签署本协议之时或之前，保密信息以合法方式属接受方所有；

（2）保密信息在通知给接受方时，已经公开或能从公开领域获得；

（3）保密信息是接受方从与其没有保密或不透露义务的第三方获得的；

（4）在不违反本协议项下约定义务的前提下，保密信息已经公开或能从公开领域获得；

（5）保密信息是接受方或其关联或附属公司独立开发，而且未从披露方或其关联或附属公司获得的信息中获益；

（6）接受方应法院或其他法律、行政管理部门要求（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序）而透露保密信息，但在该种情况发生时，接受方应立即向披露方发出通知，并作出必要说明；

9.8　保密信息披露方提供的保密信息，如涉及侵犯第三方知识产权的情况，接受方不对该等侵权行为及由此产生的索赔负责。

9.9　接受方违反本协议约定，向任意第三方泄露披露方保密信息的，披露方有权依据本协议追究其违约责任，违约金为 100,000 元人民币（大写：人民币壹拾万元整），违约金不足以弥补披露方损失的，以披露方实际损失为准。

9.10　本协议的保密期限为自本协议有效期届满之日起壹拾（10）年。

第十条　权利归属条款

10.1　本合同甲方委托乙方在技术服务中完成的技术成果的所有权益，包括但不限于知识产权及所有权，属于甲方。

10.2　乙方按照本合同约定在履行系统维护和技术服务的过程中，利用甲方提供的相关资料和工作条件完成的新技术成果的所有权益，包括但不限于知识产权及所有权，属于甲方。

10.3　在履行本合同期间，甲乙双方只能在本合同约定的范围内，经对方许可后，适当地使用对方的企业名称、商标、商号、品牌、域名和网站，双方应当尊重各自的知识

产权，不得随意改变或添加，更不得用于其他业务内容或经营目的。

10.4　双方确定，甲方有权利用乙方按照本合同约定提供的研究开发成果，进行后续改进，由此产生的具有实质性或创造性技术进步特征的新的技术成果，归甲方所有，乙方有权使用并实施。

10.5　双方确定，乙方有权在完成本合同约定的研究开发工作后，利用该研究开发成果进行后续改进。由此产生的具有实质性或创造性技术进步特征的新的技术成果，归乙方享有，经乙方同意后，甲方有权使用。

第十一条　税收条款

11.1　双方将各自承担中国有关机构根据中国税法向其征收的所有与合同执行有关的税费。

11.2　乙方应按照本合同第三条约定，对硬件设备、软件系统及技术服务分别适用13%与6%的增值税税率开具发票，并依法申报纳税。

第十二条　不可抗力

12.1　本合同所称不可抗力，是指本合同各方由于地震、台风、水灾、火灾、战争以及其他不能预见，并且对其发生和后果不能防止或不能避免且不可克服的客观情况。

12.2　本合同任何一方因不可抗力不能履行或不能完全履行本合同的义务时，应在不可抗力发生之日起的30个日历日内书面通知本合同的其他方，并在不可抗力发生之日起的90个日历日内向其他方提供由有关部门出具的不可抗力证明。

12.3　因不可抗力不能履行合同的，根据不可抗力的影响，部分或全部免除责任，但法律另有规定的除外。迟延履行合同后发生不可抗力的，不能免除责任。

12.4　如果因不可抗力的影响致使本合同中止履行90个日历日或以上时，甲方有权决定是否继续履行或终止本合同，并书面通知乙方。

第十三条　法律适用和争议解决

13.1　本合同适用中华人民共和国法律。

13.2　所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，任何一方均有权向江门市江海区人民法院提起诉讼。

第十四条　生效及其他

14.1　本合同由双方授权代表签字并加盖公章或合同专用章之日起生效。

14.2　合同将保持其有效直至双方已完全履行合同项下的所有义务并双方之间的所有付款和索赔已结清。

14.3　本合同一式肆份，甲方持贰份，乙方持贰份。

14.4　任何一方未经另一方同意不得向任何第三方透露合同内容。

14.5　对合同内容做出的任何修改和补充应为书面形式，由双方授权代表签字并加盖公章或合同专用章后成为合同不可分割的部分。

14.6　任何与本合同相关但未在合同中明确规定的事项将由双方友好协商予以解决。

14.7　甲方与乙方因执行本合同或与本合同有关的一切的通知都必须按照本合同中的地址，以书面信函形式或甲方与乙方确认的传真或类似的通讯方式进行。采用信函方式的应使用挂号信或者具有良好信誉的特快专递送达。如使用传真或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

14.8　未得到对方的书面许可，一方均不得以广告或在公共场合使用或摹仿对方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写，任何一方均不得声称对对

方的商业名称、商标、图案、服务标志、符号、代码、型号或缩写拥有所有权。

14.9　本合同中合同各方的某些义务，包括保密条款，在本合同终止或有效期之后仍对合同各方具有约束力。

14.10　本合同各章标题仅为提示之用，应以条文内容确定各方的权利义务。

14.11　如果本合同的任何条款在任何时候变成不合法、无效或不可强制执行而不从根本上影响本合同的效力时，本合同的其他条款不受影响。

14.12　双方同意，附件为协议不可分割的部分。若附件与协议正文有任何不一致,以协议正文为准。

附件一　建设清单

**说明：**

1. 各税目金额合计等于合同总价（含税价）￥_____

_____。

2. 各项产品（服务）的具体配置、功能参数以经甲方书面确认的系统设计与实施方案为准。

**一、硬件设备**

| 序号 | 产品名称 | 交付内容 | 数量 | 单位 | 单价（含 | 金额（含 |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 税） | 税） |
| | | | | | | |
| | | | | | | |

二、软件系统及技术服务

| 序号 | 产品/服务 | 交付内容 | 数量 | 单位 | 单价（含税） | 金额（含税） |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

（本页无正文）

甲方（盖章）：　　乙方（盖章）：

法定代表人或授权代表（签名）：_____　　法定代表人或授权代表（签名）：_____

日期：_____年___月___日　　日期：_____年___月___日

合同签订地点：广东省_____ 市_____区

附件 2

# 保密承诺书

致：江门市江海区政务服务和数据管理局（下称“甲方”）

为保护合作方甲方的合法利益，保证合作双方实现顺利合作，避免因信息泄露而给甲方造成损失，本项目的服务方XX（下称“承诺人”）以及参与本项目的所有员工承诺遵守本保密承诺书内容。

一、保密信息定义

本承诺书所称的“保密信息”是指所有涉密信息、商业秘密、技术秘密、通信或与该项目相关的其他信息，无论是书面的、口头的、图形的、电磁的或其他任何形式的信息，包括（但不限于）数据、用户名、口令、产品、文件、规划、方案、技术、方法、仪器设备和其他信息及文档等，上述信息在本项目中确定的形式包括但不限于：

1.甲方在项目实施中为承诺人及乙方工作人员提供必要的数据、程序、用户名、口令和资料等；

2.在对甲方提供服务工作中涉及的业务及技术文档，包括政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档，测试和测试产生的数据等；

3.服务过程中产生的所有成果为保密的内容；

4.其他甲方合理认为并申明属于保密信息的内容。

二、保密要求

承诺人在国家相关法律法规、规章政策所规定的前提下，全力限制“保密信息”的使用范围以利保密防范，并仅用于为甲方提供服务。在未经甲方书面形式授权下，承诺人不会直接或间接使用保密信息，亦不会把任何保密信息披露给他人，承诺人的所有员工均有义务受约束，并负有保密的义务。

1.承诺人始终对保密资料保密，不在项目之外使用甲方提供的保密信息及因履行本项目而掌握的保密信息。

2.未经甲方书面同意，不向任何第三方提供保密信息以及可以接触上述保密信息的手段，包括在公开场合展览，公开对外宣传，作为文章、讯息、参考数据发表等。

3.在接触内部网络管理数据时，认真学习和遵守甲方相关规定。不私自下载、拷贝计算机内的秘密和敏感信息；不将信息系统的程序、口令、密钥等泄露给无关人员；不擅自携带记载工作内容的硬盘、软盘和打印资料外出。

4.只向项目相关人员（包括各自的领导、同事和雇员等）为商讨合作项目而有需要知悉保密信息的人士披露保密信息；并保证上述各相关人员的行为将会符合本守则的规定。

5.在商讨合作项目的过程中，若需向第三方披露甲方的保密信息，应取得甲方书面许可，并要求该第三方不得向任何其他人士泄露保密信息。

6.有关保密的内容和义务，未经甲方解封则长期有效。

承诺人:

（法定代表人或委托代理人签字并盖单位公章）

日　期：

附件 3

# 廉洁从业承诺书

为规范双方在项目合作期间的廉洁从业行为，建立公开、公平、公正、诚信的合作关系，防范商业贿赂与廉政风险，保障国家利益、公共利益及双方合法权益，采购单位（以下简称“甲方”）与乙方（合作供应商）本着平等自愿原则，共同作出如下双向廉洁承诺，本承诺书作为双方已签署项目合同的补充文件，与主合同具有同等法律效力。

一、双方共同遵守条款

严格遵守《中华人民共和国政府采购法》《中华人民共和国反不正当竞争法》《中华人民共和国招标投标法》等国家相关法律法规，以及双方各自的廉政建设、采购管理规章制度，共同恪守公开透明、诚实守信、廉洁自律的合作原则。

建立常态化廉洁沟通机制，双方指定专人作为廉洁从业监督联系人，对合作过程中发现的不廉洁苗头第一时间相互提醒、及时纠正，对涉嫌违规违纪的线索直接向对方纪检监察部门举报。

自觉接受纪检监察、财政、审计等监管部门的监督检查，如实提供相关资料，不隐瞒、不伪造、不篡改采购及履约全流程档案资料。

双方人员不得利用职权或业务便利，向对方提出任何与本次合作无关的私人利益诉求，不得借业务往来谋取不正当好处。

二、采购单位（甲方）廉洁承诺

严格执行法定采购程序，不设置倾向性、排他性采购条款，

不指定特定品牌、供应商或技术参数，不对乙方及其他潜在供应商实行差别或歧视待遇。

绝不向乙方索要或收受礼金、有价证券、贵重物品、回扣、好处费等财物，不要求乙方报销应由甲方个人支付的任何费用。

不接受乙方安排的可能影响公平公正交易的宴请、旅游、健身、娱乐等活动，不要求乙方为甲方人员的住房装修、婚丧嫁娶、家属就业、子女入学、出国出境等事项提供便利。

不泄露采购涉密信息，不私下接触乙方人员串通干预评审结果，不与乙方签订“阴阳合同”擅自变更项目核心条款，不无故拖延项目款项支付。

严格执行利益冲突回避规定，甲方参与本项目的所有人员，若与乙方存在亲属关联、持股任职等利害关系，必须主动申请回避。

三、乙方（合作供应商）廉洁承诺

坚持诚信经营，不采取围标、串标、弄虚作假等不正当手段谋取合作机会，不向甲方工作人员打探招标响应、采购决策等保密信息，不干扰正常采购与履约流程。

绝不以任何名义向甲方工作人员（含其配偶、子女、亲属及其他共同利益关系人）赠送礼金、礼品、有价证券、股份等财物，不以任何形式向甲方人员输送不正当利益。

不为甲方人员安排可能影响公正履职的宴请、旅游、娱乐等活动，不为甲方人员的个人消费事项提供支付便利，不向甲方人员输送任何形式的商业贿赂。

严格按照主合同约定的质量标准、交付时限、服务要求履

约，不降低产品服务标准、不以次充好，不通过欺诈手段谋取不正当利益。

已对本单位参与本项目的所有人员完成廉洁从业教育，对相关人员的行为承担全部管理责任；若发现甲方人员存在索要贿赂等违规行为，第一时间向甲方纪检监察部门举报，并配合调查取证。

四、违约责任与生效约定

若甲方人员违反上述承诺，甲方将按党纪政纪相关规定对责任人严肃处理，涉嫌违法犯罪的移交司法机关追究法律责任，同时向乙方公开反馈处理结果。

若乙方违反上述承诺，甲方有权采取以下一项或多项处置措施：立即终止或解除主合同、将乙方纳入供应商廉洁黑名单并在 1-3 年内禁止参与甲方所有采购活动、不予支付或追回已支付的全部合同款项、要求乙方赔偿甲方因此遭受的全部经济损失；涉嫌违法犯罪的，移交司法机关追究法律责任。

本承诺书自双方法定代表人或授权代表签字并加盖公章之日起生效，有效期覆盖本项目采购、履约、验收、款项支付全流程，直至项目质保期届满为止。

（以下无正文，为签署页）

甲方（采购单位）：（盖章）

法定代表人/授权代表签字：

日期：_____年____月____日

乙方（供应商）：（盖章）

法定代表人/授权代表签字：

日期：_____年____月____日