# 省体育局二沙体育训练中心协同办公平台升级改造
# （2025年）项目密码安全测评服务
# 采购需求书

项目需求

△1.项目业主：广东省二沙体育训练中心

△2.采购项目名称：省体育局二沙体育训练中心协同办公平台升级改造(2025年)项目密码安全测评服务

△3.是否为行政管理的中介服务项目采购：否

△4.投资审批项目：否

△5.**项目规模：4万**

△6.所需服务：信息系统项目密码安全测评服务（检验检测服务）

△7.服务时限说明：服务期限自双方签订合同生效起到服务内容通过最终验收为止。

△8.服务内容：

**一、项目名称：**省体育局二沙体育训练中心协同办公平台升级改造(2025年)项目密码安全测评服务

**二、项目地址：**广东省广州市越秀区大通路28号

**三、项目采购内容：**本次采购内容为省体育局二沙体育训练中心协同办公平台升级改造(2025年)项目密码安全测评服务

**四、密码安全测评服务内容包含且不限于：**

**1.测评服务目标**

为保障省体育局二沙体育训练中心政务信息系统的运行安全，密码应用符合国家的相关标准，在项目全过程中考虑商用密码应用合规性，系统建设完成后需要按照相关的要求进行商用密码的测评，保证各项改造符合商用密码的应用安全要求。

**在密评活动结束30个工作日内，将评估结果报密码管理部门等相关部门备案。**

**2.评估内容**

组织获得国家商用密码应用安全性评估认证资质的安全测评机构对省体育局二沙体育训练中心政务信息系统进行系统评估、协助指导安全整改，最终输出被评估系统商用密码应用安全性评估报告（含整改或者建设建议），满足商用密码应用安全性评估工作的验收要求，具体内容包括：

| 序号 | 服务内容 | 服务内容子项 | 工作内容 |
|---|---|---|---|
| 1 | 需求沟通确认 | 需求沟通调研和确认 | 对安全评估的组织实施流程、风险管控效果、 |

| 序号 | 服务内容 | 服务内容子项 | 工作内容 |
| --- | --- | --- | --- |
| | | 工作实施要求 | 时间节点、交付成果、评估方式等基础信息进行沟通核实，确认服务需求和工作要求 |
| 2 | 基础材料搜集整理和现场沟通采集 | 按照评估准备实施要求，搜集整理必要素材 | 通过远程或现场会议方式与业务研发、运维部门技术团队和保障团队沟通评估所需基础素材、文档等必要信息 |
| 3 | 差距评估组织实施 | 依据(GB/T 39786-2021)《信息安全技术信息系统密码应用基本要求》等标准进行测评 | 采取材料审查、人员访谈、实地查看、配置检查、工具测评等评估方法对系统密码应用情况进行评估分析，核查系统技术应用、密钥管理、安全管理是否符合密评要求 |
| 4 | 制定评估整改建议 | 制定整改建议，明确具体措施、效果要求 | 根据差距评估结果，结合密码应用法律法规、政策标准及风险管控要求，提出评估意见和整改建议，指导系统集成商对被测系统按照(GB/T 39786-2021)《信息安全技术信息系统密码应用基本要求》进行整改 |
| 5 | 验收评估（复评） | 对整改完成后的系统进行评估 | 对整改完成后的系统，按照(GB/T 39786-2021)《信息安全技术信息系统密码应用基本要求》及评估通过的密码应用方案进行评估，给出最终评估结论 |

**3.评估依据**

（1）《中华人民共和国密码法》

（2）《中华人民共和国网络安全法》

（3）《商用密码管理条例》

（4）《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）

（5）《商用密码应用安全性评估管理办法（试行）》

（6）《信息系统密码测评要求》（试行）

（7）《商用密码应用安全性评估测评过程指南》（试行）

（8）《商用密码应用安全性评估测评作业指导书》（试行）

（9） 通过评审的被测系统密码应用方案

**4.评估对象**

测评对象主要为省体育局二沙体育训练中心协同办公平台升级改造(2025 年)项目中关联的相关应用系统。

**5.评估流程**

密码应用安全性评估过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。

（1）评估准备阶段

根据被测系统规模，测评机构组建测评项目组，从人员方面做好准备。测评机构应派出**通过商用密码应用安全性评估人员测评能力考核的测评人员**承担测评工作，未通过测评考核的测评人

员不得参与测评工作，保证测评工作符合国家商用密码应用安全性评估有关工作要求。测评机构通过调研表调研、现场调研、查阅被测系统已有资料等方式，了解整个系统的构成和商用密码保护情况，为编写测评方案和开展现场测评工作奠定基础。测评项目组成员在进行现场测评之前，熟悉与被测系统相关的各种组件、调试测评工具、准备测评过程中需使用的各类表单等。

（2）方案编制阶段

根据调研获取的被测系统信息，测评机构分析整个被测系统及其涉及的业务应用系统，以及与此相关的商用密码应用情况，确定本次测评的测评对象。根据被测系统备案情况和重要性分析，确定本次测评的测评指标。测评过程中，确认现场测评的关键安全点，并充分考虑测评的可行性和风险，最低限度的避免对被测系统，尤其是在线运行业务系统的影响。确定现场测评的具体实施内容，完成测评方案的编制。

（3）现场评估阶段

测评项目组根据测评方案以及现场测评准备的结果，安排测评人员在现场完成测评工作，汇总现场测评的测评记录。测评双方对测评过程中发现的问题进行现场确认；测评机构归还测评过程中借阅的所有文档资料。

（4）分析与报告编制阶段

在现场测评工作结束后，测评机构对现场测评获得的测评结果进行汇总分析，形成测评单元测评结果后，进而进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成测评结论。

**6.评估指标**

针对省体育局二沙体育训练中心的信息系统，开展商用密码应用安全性评估，从总体要求、物理和环境、网络和通信、设备和计算、应用和数据、密钥管理、安全管理等方面开展测评，具体测评指标包括但**不限于如下指标（参考《省体育局二沙体育训练中心协同办公平台升级优化(2025 年)项目密码应用方案》）：**

| 技术/管理 | 安全分类 | 指标要求 |
|---|---|---|
| 总体要求 | 密码算法 | 使用的密码算法应当符合法律、法规的规定和密码相关国家标准、行业标准的有关要求； |
| | 密码技术 | 使用的密码技术应遵循密码相关国家标准和行业标准； |
| | 密码产品 | 使用的密码产品与密码模块应通过国家密码管理部门核准； |
| | 密码服务 | 使用的密码服务应通过国家密码管理部门许可。 |
| 技术要求 | 物理和环境安全 | a）应使用密码技术的真实性功能来保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性； |
| | | b）应使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性； |
| | | c）应使用密码技术的完整性功能来保证视频监控音像记录的完整性； |
| | | d）宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| | 网络和通信安全 | a）应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性； |
| | | b）应使用密码技术的完整性功能来保证网络边界和系统资源访问控制 |

| 技术/管理 | 安全分类 | 指标要求 |
| --- | --- | --- |
| | | 信息的完整性； |
| | | c）应采用密码技术保证通信过程中数据的完整性； |
| | | d）应采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性； |
| | | e）应采用密码技术建立一条安全的信息传输通道，对网络中的全设备或安全组件进行集中管理； |
| | | f）宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| | 设备和计算安全 | a）应使用密码技术对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| | | b）在远程管理时，应使用密码技术的机密性功能来实现鉴别信息的防窃听； |
| | | c）应使用密码技术的完整性功能来保证系统资源访问控制信息的完整性； |
| | | d）应使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性； |
| | | e）应采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护； |
| | | f）应使用密码技术的完整性功能来对日志记录进行完整性保护； |
| | | g）宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| | 应用和数据安全 | a）应使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性； |
| | | b）应使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性； |
| | | c）应采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等； |
| | | d）应采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等； |
| | | e）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等； |
| | | f）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息、重要可执行程序等； |
| | | g）应使用密码技术的完整性功能来实现对日志记录完整性的保护； |
| | | h）应采用密码技术对重要应用程序的加载和卸载进行安全控制； |
| | | i）宜采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。 |
| 密钥管理 | 密钥生成 | a)密钥生成使用的随机数应符合GM/T 0005要求，密钥应在符合GM/T 0028的密码模块中产生；密钥应在密码模块内部产生，不得以明文方式出现在密码模块之外；应具备检查和剔除弱密钥的能力。 |
| | 密钥存储 | a)密钥应加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥应存储在符合GM/T0028的二级及以上密码模块中。 |
| | 密钥使用 | a)密钥应明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前应对其进行验证；应有安全措施防止密钥的泄露和替换；密钥泄露时，应停止使用，并启动相应的应急处理和响应措施。应按照密钥更换周期要求更换密钥；应采取有效的安全措施，保证密钥更换时的安全性。 |

| 技术/管理 | 安全分类 | 指标要求 |
| --- | --- | --- |
| | 密钥分发 | a)应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。 |
| | 密钥导入与导出 | a)应采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。 |
| | 密钥备份与恢复 | a)应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。 |
| | 密钥归档 | a)应采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施 |
| | 密钥销毁 | a)应具有在紧急情况下销毁密钥的措施。 |
| | | b) 事件发生后，应及时向信息系统的上级主管部门进行报告； |
| | | c) 事件处置完成后，应及时向同级的密码主管部门报告事件发生情况及处置情况。 |

**7.评估方法及工具**

1）现场测评方法

商用密码应用安全性评估使用的测评方法包括：

（1）访谈：访谈涉及总体要求、物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理和安全管理等方面内容。通过与被测单位的相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认。

（2）文档审查：审核被测单位提交的有关信息系统安全的各个方面的文档，如：被测系统总体描述文件，被测系统商用密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，密码应用方案及评审意见，自查或上次评估报告等等。通过对这些文档的审核与分析确认测评的相关内容是否达到相应安全保护等级的要求。

（3）实地查看：现场查看测评对象所处的环境、外观等情况。

（4）配置查看：查看测评对象的相关配置。

（5）工具测试：根据被测单位信息系统的实际情况，测评人员使用端口扫描、数据捕获、协议分析和代码走查等适合的技术或工具对信息系统进行测试。

2）测评工具

在商用密码应用安全性评估中使用的评估工具严格遵循可控性原则，即所有使用的测评工具需事先提交给系统建设单位检查确认，确保在双方认可的范围之内，而且测评过程中采用的技术手段确保已经过可靠的实际应用。

**8.输出文档**

测评机构评估完成后，最终输出省体育局二沙体育训练中心协同办公平台升级改造(2025 年)项目的密码应用安全性评估报告，**并由评估机构协助将评估结果报广东省密码管理局备案**。成果清单包括但不限于：

| 序号 | 交付文档 | 备注 |
| --- | --- | --- |
| 1 | 《密码应用安全性评估报告》 | 纸件、电子件 |

**五、质量要求：**

成交人应严格依据《中华人民共和国密码法》《商用密码管理条例》及国家、省、市现行有效的密码安全技术规范与密码测评标准（含 GB/T 39786《信息安全技术 信息系统密码应用基本要求》等），结合采购人信息系统的实际密码应用定级情况与密码安全需求，采用科学严谨、客观公正的测评方法和技术手段，对密码安全测评全过程实施规范化质量管理

测评过程应科学合理、方法先进、记录完整，确保测评结果真实可靠、问题定位精准。并严格遵守各项规章制度和廉政纪律、保密规定和工作要求，全程接受采购人的监督和管理。

**六、报价人资格要求：**

报价人须满足以下要求并在成交候选时根据采购人通知提供以下纸质版资料：

1.报价人必须是具有独立承担民事责任能力的在中华人民共和国境内注册的法人或其他组织或自然人。

2.报价人必须具有良好的商业信誉和健全的财务会计制度且有依法缴纳税收和社会保障资金的良好记录。

3.报价人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。

4.★报价人必须是在中华人民共和国境内注册、具有独立承担民事责任能力的法人或其他组织（提供有效的营业执照或事业法人登记证等副本复印件），并具有国家密码管理局颁发的《商用密码检测机构资质证书》。

5.报价人必须符合法律、行政法规规定的其他条件。

6.本项目不接受备选方案，不接受联合体报价。

**七、人员配置要求：**

★报价人应为本项目成立相应的密码安全测评服务组，并指定专职的项目责任人负责项目协调和调度工作，项目组成员不得少于 3 人，其中项目责任人 1 名，应具有具有国家商用密码应用安全性评估人员测评能力考核小组颁发的商用密码应用安全性评估从业人员考核合格证书、具有 5 年及以上商用密码评估方面工作经验；测评工程师不少于 2 名，具有 1 年以上信息化项目密码安全测评服务经验，工作年限以在测评单位工作期间缴纳的社保年限为准。投标时须提供团队成员相关证件、就职证明文件及业绩文件复印件。

成交人不允许随意更换项目负责人，如确需更换，须事前征得采购人同意，且变更人员的业务能力、资质水平不得低于被更换人员。如成交人派出的人员未按合同履行职责，或不服从工作安排，不满足工作要求，或与第三方串通造成经济损失等情形的，成交人应在接到采购人通知后予以撤换，所调换人员的业务能力、资质水平不得低于投标(响应)文件中所承诺人员的素质。

**八、付款方式：**

本项目分两笔支付。

1、第 1 期：双方正式签订合同并生效后，采购人在 10 个工作日内向成交人支付合同总价的

50%。

2、第 2 期：项目最终验收通过后 10 个工作日内，采购人向成交人支付合同总金额的 50%。

3.本项目的付款时间是指采购人向政府采购支付部门提出付款申请的时间，不含其审核和支付的时间；

4.付款方式：采用银行转账、银行汇付（含电汇）等形式；

5.每期支付合同款项时，成交人需提前 5 天向采购人提供与当期支付款项金额等值的中国大陆地区合法有效发票。

**九、其他说明：**

1.成交人不许转包，不许擅自分包。

2.报价人应承担所有与编写和提交报价文件有关的费用，不论报价的结果如何，采购人在任何情况下均无义务和责任承担这些费用。

3.双方签订合同后，若因采购人原因造成项目停止建设的，成交人应无条件服从，不得以任何理由向采购人提出任何形式索赔。

4.本项目采购方式：方案择优方式。