采购需求

一、机关协同办公平台密改服务主要内容：

密码改造工作（以下简称“密改”）是提升信息系统安全性的重要举措，涉及密码策略的更新、密码技术的改进以及密码管理流程的完善等多个方面。根据《密码法》《密码强国建设纲要》《机要密码工作条例》《商用密码管理条例》《西安市商用密码应用安全性评估暂行办法》等有关规定，网络安全等级保护三级以上的信息系统须进行密码改造。

我委机关目前在用自建的6个系统中，网络安全等级保护三级以上的是机关协同办公平台（以下简称“OA系统”）（办公室）和市重点产业企业库（高技术处）。为有序推进密改工作，结合系统的使用频次、紧急程度、数据敏感度等因素，并考虑工作需求和“过紧日子”要求，2023年底，我委向市数据局、市财政局申请将OA系统作为今年密改对象。同时，鉴于OA系统是我委的“信息中枢”，为确保该系统符合各方管理要求，提升安全性、可用性，此次改造拟同步实施信创改造，并集成对接“秦政通”平台，改造内容主要包括以下几个方面；

二、服务主要内容：

（1）OA系统的信创适配；

将OA系统的应用服务迁移部署至市数据局信创云平台环境下，完成协同办公OA系统的X86环境到国产化信创环境适配开发及改造，满足信创要求。同时兼顾客户端X86环境和国产化信创环境的“双生态”运行，平滑过渡，达到无感知切换升级

（2）信创环境下密码机制改造；

综合考虑市数据局信创云平台环境下OA系统物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的信创环境下密码应用方案，满足《基本要求》中三级指标要求，为通过密码应用安全性评估奠定基础。该项目密码应用框架模型由密码技术体系和密码应用管理体系2部分组成，通过双轨驱动，满足国产信创环境下的密码机制要求

（3）与“秦政通”进行集成对接；

“秦政通”是省政务数据局统一开发的政务一体化协同办公平台，按照远期规划，全省各级都要通过“秦政通”处理日常公务。各单位已建的办公系统应坚持“应接尽接”原则，通过适配改造方式逐步整合至“秦政通”。本次拟将信创环境下的OA系统对接到“秦政通”平台，实现公文收发办理、人员信息认证等有关功能与“秦政通”平台相集成。

三、人员岗位要求

供应商应提供专业的技术团队常驻现场进行运维，运维服务团队人员应包含项目经理、运维工程师。

1、项目经理岗位职责

根据项目要求组建项目团队；

根据项目情况、要求制定行之有效的项目计划；

领导项目组按计划开展项目运作，保证项目进度符合双方要求；

负责项目质量，保证项目质量符合客户要求；

协调项目实施过程中与客户的关系，保证项目顺利开展；

定期向甲方项目领导汇报项目进度、项目情况，进行风险预测与评估，保证项目效果；

参与项目的全过程；

工作主要包括：

（1）组建项目小组；准备项目环境；与客户项目负责人根据现实情况谈论决定实际的项目计划；

（2）进行相关的需求调研，调研内容包括：组织结构、现有应用系统、当前系统软件配置、基本数据环境(包括存储策略、安全策略、备份策略、灾难恢复策略)、用户情况、公文处理需求、协同需求、常用办公功能需求、其它需求。完成需求确认；

（3）根据调研情况实现应用，包括系统的配置、流程设计、模板设计等；根据调研情况对特定系统进行二次开发；

（4）对实现的功能进行测试，检验：是否符合需求、是否存在bug、系统性能问题等；

（5）集中培训客户系统管理员与应用管理员，使管理员具有系统维护和管理的技能，能快速定义各种类型的公文以及流程，进行系统用户管理和维护；协助客户管理员进行普通用户的培训，包括领导层、各处室领导及一般工作人员；培训内容包括系统的基本操作方法，收文和发文的处理形式、文档的查询、其它办公模块的使用等；

四、其他要求

1、制度要求

良好的管理制度，严密的组织实施计划，严格的监督检查机制对保证项目的成功至关重要。

决策制度：对于项目实施过程中的日常工作，一般由项目经理加以决策，然后提交给项目领导小组、乙方项目实施组和项目经理，一般在2 天之内，如果没有任何一方提出异议，则该决定生效，此异议应以书面方式表达。一切决策应有书面文件，并且在项目文档管理组备案。

交流制度：所有项目组成员，如发现项目进展隐患，应及时向项目经理或其他人员提醒。提醒可以以书面或口头方式。

例会制度：每周五下午及每月最后一周的末尾工作日，由项目经理组织在现场的双方项目组成员参加周/月例会。总结上周/月工作，形成项目周/月报。项目周/月报的内容包括：上周/月工作进展报告、本周/月工作计划、本周/月任务分派报告。

问题争议制度：在项目中，任何不能达成一致的观点均为争议，争议应立即向项目的上级单位呈报，并报项目管理部。争议应由可以协调争议各方的机构加以裁决，并对裁决承担责任。争议裁决人由项目管理部项目经理选择。争议的最高仲裁机构为项目领导决策组。

2、安全服务要求

应满足国家信息系统安全等级保护要求，依据所定安全等级要求进行安全等保的规划与建设，从物理安全、网络安全、主机安全、应用安全和数据安全几个层面制定安全保护措施。在访问控制、安全审计、通信完整性与保密性、抗抵赖、软件容错等方面保障系统应用安全。

（1）故障服务响应

|  |  |  |
| --- | --- | --- |
| 故障级别 | 到达现场时间 | 解决时间 |
| 一级故障：系统崩溃或系统性能严重下降，业务系统无法正常运行 | 30分钟内提供电话支持， 1小时内到达现场 | 到达现场后的4小时内 |
| 二级故障：系统性能有一定下降，业务系统受到干扰 | 30分钟内提供电话支持，4小时内到达现场 | 到达现场后的8小时内 |
| 三级故障：系统可以运行，但系统有不明原因的报错 | 30分钟内提供电话支持，8小时内到达现场 | 到达现场后的24小时内 |

（2）应急预案

1、病毒安全紧急处置措施：

当发现有计算机被感染上病毒后，应立即向信息系统管理技术人员报告，将该机从信息系统上隔离开来信息系统管理技术人员在接到通知后，应在三十分钟内响应。对该设备的硬盘进行数据备份。用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。如果现行反病毒软件无法清除该病毒，应立即向应急处理工作小组组长报告，并迅速联系有关产品商研究解决。应急处理工作小组经会商，认为情况严重的，应立即向应急处理领导小组组长汇报。应急处理领导小组经会商后，认为情况极为严重的，应立即向公安部门或上级机关报告。如果感染病毒的设备是中心服务器系统，经领导小组同意，应立即告知各相关部门做好相应的清查工作。

2、数据库安全紧急处置措施

主要数据库应按双机热备设置，并至少要准备两个以上数据库备份，平时一个备份放在机房，另一个备份放在另一个安全的场所。一旦数据库崩溃，应立即启动备用系统，并向应急处理工作小组组长报告。在备用系统运行期间，业务系统技术人员应对主机系统进行维修。如果两套系统均崩溃，业务系统技术人员应立即向应急处理工作小组组长报告，应急处理工作小组如认为情况严重，应立即向应急处理领导小组组长汇报。同时通知相关科室部门暂缓使用业务系统和上传上报数据。系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库加已恢复。如果两个备份均无法恢复，应立即向应急处理工作小组组长汇报，并向有关厂商请求紧急支援。

3、软件系统遭破坏性攻击的紧急处置措施

重要的业务系统必须存有备份，与业务系统相对应的数据必须有多日的备份，并将他们保存在安全处。一旦信息系统遭到破坏性攻击，应立即向信息系统管理技术人员、业务系统技术人员报告，并将该系统停止运行。信息系统管理技术人员检查日志等资料，确定攻击来源。由业务系统技术人员向应急处理工作小组组长汇报。应急处理工作小组组长认为情况严重的，应立即向应急处理领导小组汇报。应急处理领导小组认为情况极为严重的，应立即向公安部门或上级机关报告。

五、保密要求

1、供应商应完全按照国家有关保密法律法规、标准和甲方 的要求，对甲方委托的实施服务全过程进行保密管理；

2、供应商不得将保密范围内的任何信息或实物等向第三方出售、出租、外借、转让、转包、泄露或以其他形式提供；

3、保密范围内的信息或实物等归甲方所有，供应商只能在合作范围内使用，不得利用甲方的信息从事营利活动

六、测评与考核管理

根据单位内部情况设定测评与考核模式：测评管理包括设定测评方式、测评人设定、测评时间、测评等级、测评百分比等；考核管理包含季度考核、年度考核、集体考核、考核流程与表单管理、考核结果统计与查询和人员基础信息管理。同时对于测评及考核管理支持过程管理和进度追踪，支持数据推送至人事处并进行统计分析。