江苏省政府采购合同（服务）（合同编号）

项目名称：省国资委政务信息系统迁移上云及改造项目

项目编号：JSTCC26022101967（JSZC-320000-JITC-G2026-0093）

甲方：江苏省政府国有资产监督管理委员会

乙方：江苏省数据集团数字科技有限公司

甲、乙双方根据省国资委政务信息系统迁移上云及改造项目公开招标的结果，签署本合同。

一、合同内容

1.1 服务内容：对照国家、省级政务信息化工作决策部署及省委省政府“一部门一系统”集约化建设要求，我委信息化以“系统变革、整体重塑”为原则，解构现有信息系统，对数字化整体架构进行优化，完成信息系统国产化改造、信息系统集成整合、信息系统迁移上云、数字化架构优化、安全保障加固工作以及电子政务平台（OA）集成，以全面提升监管服务能力。（具体详见附件 2《采购需求》）

1.2 服务期限：自合同签订之日起 8 个月。

1.3 补充条款：无

1.4 下列文件均为本合同的组成部分：

（1）招标文件；

（2）投标文件；

（3）中标通知书；

（4）合同附件与合同有关的其它资料。

二、合同金额

2.1 本合同金额为（大写）： 贰佰零玖万捌仟元（2098000 元）人民币，（发票含税，上述费用已包含乙方为全面履行本合同的所有费用），税率为 6 %。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的货物）的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向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的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任，同时，乙方应全额赔偿甲方因此遭受的全部损失，包括但

不限于：甲方支付给第三方的赔偿金、诉讼费、律师费、保全费及其他合理维权费用；甲方因侵权纠纷被迫更换、重作所产生的直接及间接损失；以及甲方为消除侵权影响、应对舆情所支出的全部费用。甲方有权在应付乙方款项中直接抵扣上述赔偿金及费用，不足部分乙方应在甲方通知后三日内补足。

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约承诺

6.1 履约保证金：本项目不收取履约保证金。

6.2 履约承诺：乙方遵循甲方的技术指导和调配，接受甲方对代码编写的规范和管理，并以科学方法进行实施。

6.3 乙方承诺具备签订本合同、从事本合同项下技术服务的合法资质和技术能力。

6.4 乙方承诺，投标文件中所列明的项目负责人及核心技术骨干为本项目服务的常驻人员，在项目最终验收前，未经甲方书面同意，乙方不得擅自更换。甲方认为乙方指派的技术服务人员（包括但不限于项目负责人）无法满足甲方服务要求的，有权要求乙方在 5 个工作日内予以更换，且新更换人员的资质和经验水平不得低于被更换人员。逾期未更换或更换后仍不符合要求的，每发生一次，乙方应向甲方支付合同总金额 2%的违约金。

6.5 本项目自最终验收合格之日起，乙方提供一年的免费质保服务。质保范围为：确保本合同项下所有系统（包括迁移改造后的系统及新建功能）能够稳定、正常运行，达到附件约定的性能、功能及安全指标。质保期内，任何因乙方工作成果导致的质量问题、性能瓶颈、安全漏洞或故障，乙方均应按第 13.4 条约定免费修复、维护及提供技术保障。

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方不得将合同标的分包给他人履行。

7.3 乙方如有转包或分包行为，甲方有权解除合同。

八、交付方式及交付地点

8.1 交付方式：现场交付

8.2 交付地点：南京市玄武区中山路 338 号苏粮国际大厦

九、合同款项支付

9.1 签订合同且系统上线运行并通过甲方组织的集成测试后支付合同金额的 50% ，系统上线运行稳定且项目整体通过最终验收后支付合同金额的 50% 。

9.2 甲方通过转账方式支付费用，乙方用于接收合同款项的账户信息如下：

账户名：江苏省数据集团数字科技有限公司

开户银行：建行南京中山南路支行

银行账号：32050188123600000187

9.3 付款前，乙方开具符合国家规定的发票，甲方收到发票后30日内进行支付，如因乙方未及时开具发票或开具发票不符合要求，造成甲方逾期付款的，甲方对此不承担任何责任。

十、税费

本合同执行中相关的一切税费均由乙方负担。

十一、质量保证及售后服务

11.1 乙方应按招标文件规定和响应文件承诺的性能、技术要求、质量标准向甲方提供服务。

11.2 乙方提供的服务在服务期内因其本身出现质量问题，根据实际情况，经双方协商，可按以下办法处理：

（1）更换：由乙方承担更换费用。

（2）解除合同，甲方退回产品和服务，乙方退还甲方支付的全部款项并赔偿甲方全部损失。

11.3 如在使用过程中发生质量问题，乙方经甲方通知，在约定时间内未派人到达甲方现场处理，或虽经处理，但未能解决出现的服务质量和安全问题，甲方有权委托第三方处理，甲方委托第三方处理的费用由乙方承担。

11.4 在服务期内，乙方应对服务出现的质量及安全问题负责处理解决并承担相应费用。

11.5 合同标的对质量保证和售后服务另有要求的，按招标文件中的相关要求处理。

十二、验收

12.1 甲方依法组织履约验收工作。

12.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

12.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

12.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

12.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时，甲方按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，验收小组出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付条件挂钩。履约验收的各项资料存档备查。

12.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

12.7 最终验收应以本合同、附件 2《服务要求》、中标通知书、乙方投标文件以及双方确认的实施方案为共同依据。甲方将依据附件 2 中“二、技术要求”、“五、功能要求”所列明的各项量化指标（包括但不限于常规网页加载时间≤1 秒、国产化替换率 100%、核心数据迁移准确率 100%、平均年故障时间<1 天等）进行逐项测试和确认。任何一项指标不符合约定的，甲方有权认定验收不合格。

十三、违约责任

13.1 本合同生效后，甲乙双方应本着诚实信用原则，严格履行本合同约定的各项义务。如果乙方不履行本合同约定义务的，或者履行义务不符合约定的，均视为违约，应向甲方支付合同总额百分之五的违约金。除本合同另有约定外，乙方还应向甲方赔偿因此遭受的损失，包括但不限于直接损失以及由此而产生的律师费、诉讼费、保全费、公证费、交通费等合理费用。

13.2 因乙方原因造成甲方设备损坏的，乙方应进行修理、更换并赔偿甲方因此遭受的损失。

13.3 乙方逾期完成服务的，乙方应按服务合同总额每日千分之六向甲方支付违约金，由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工作日不能完成服务的，甲方可解除本合同。乙方因逾期完成服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同价款总额百分之五的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

13.4 在质保期内（自验收合格之日起 1 年），系统出现功能缺陷、性能不达标、故障时，按照招标文件可靠性指标要求由乙方免费进行修复。乙方应在接到甲方通知后 48 小时内完成修复，逾期未修复或无法修复的，应当向甲方支付合同价款总额 百分之五 的违约金，如乙方支付的违约金不足以弥补甲方损失（包括但不限于甲方找第三方修复或重做的费用、因系统故障给甲方造成的其他损失等），超出部分由乙方继续承担赔偿责任。

13.5 乙方所提供服务的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

13.6 项目最终验收时或质保期内，经甲方或甲方委托的第三方检测机构认定，乙方交付的工作成果不符合本合同附件《服务要求》中约定的关键性能指标、国产化率、安全标准或数据准确性要求的，视为乙方根本违约。甲方有权要求乙方在指定期限内无偿整改；逾期未整改或整改后仍不达标的，甲方有权单方解除合同，并要求乙方支付合同总金额 10% 的违约金，同时乙方应退还甲方已支付的全部款项，并赔偿甲方因此遭受的全部损失。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期延长，其延长期与不可抗力影响期相同。

14.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十五、解决争议的方法

15.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。

十六、保密

双方应对在合同履行过程中所获得的对方的相关信息承担保密义务，具体要求详见附件 1：《保密协议》。该约定在本合同终止后仍然继续有效，且不受合同解除、终止或无效的影响。

十七、合同生效及其它

17.1 合同经双方签字并加盖单位公章或合同章后生效。

17.2 本合同未尽事宜，遵照中华人民共和国现行法律法规有关条文执行。

17.3 本合同正本一式肆份，具有同等法律效力，甲乙双方各执两份。

（本页以下无正文）

甲方：江苏省政府国有资产监督管理委员会

地址：南京市玄武区中山路 338 号苏粮国际大厦

法定代表人或授权代表：

联系电话：

签订日期：2026 年 6 月 12 日

乙方：江苏省数据集团数字科技有限公司

地址：南京市建邺区庐山路 168 号 9 楼 912-16 室

法定代表人或授权代表：

联系电话：18021391758

签订日期：2026 年 6 月 12 日

附件 1：

保密协议

甲方：江苏省政府国有资产监督管理委员会

乙方：江苏省数据集团数字科技有限公司

甲乙双方经友好协商，根据《中华人民共和国民法典》及相关法律法规的规定，就乙方在合同履约过程中可能获悉的甲方保密信息及为甲方保密事宜，达成如下协议：

1.本协议所称“保密信息”是指：乙方基于为甲方提供服务所获取的甲方域名、业务系统等虚拟资产中所附带的或甲方安全设备上报的网络安全信息， 以及用户数据和业务相关信息等。

2.未经甲方书面同意，乙方不得以任何形式或任何方式将保密信息和/或其中的任何部分，披露或透露给任何第三方。乙方有义务妥善保管保密信息，不得擅自复制备份，并应避免泄露或遗失。乙方亦不得依据保密信息，就任何问题，向任何与甲方所需安全服务无关的第三方做出任何建议。

3.甲方同意乙方有权因提供服务的必要，而向其安全服务人员透露或允许其接触保密信息和/或其中的任何部分，同时，乙方承诺该等服务人员在提供服务的过程中将对其所接触的保密信息承担与本协议同等的保密义务。

4.甲方有权在服务终止时要求乙方将所获悉的保密信息归还给甲方，不能归还的，应进行销毁处理。

5.凡因执行本协议所发生的或与本协议有关的一切争议，甲乙双方应通过友好协商解决。如果协商不能解决时，甲乙双方同意向甲方所在法院提起诉讼。

6.本协议保密期限为永久保密。

7.本协议一式贰份，自甲乙双方盖章之日起生效。

（本页以下无正文）

甲方：江苏省政府国有资产监督管理委员会

地址：南京市玄武区中山路 338 号苏粮国际大厦

法定代表人或授权代表：

联系电话：

签订日期：2026 年 6 月 12 日

乙方：江苏省数据集团数字科技有限公司

地址：南京市建邺区庐山路 168 号 9 楼 912-16 室

法定代表人或授权代表：

联系电话：18021391358

签订日期：2026 年 6 月 12 日

附件 2：

采购需求

对照国家、省级政务信息化工作决策部署及省委省政府“一部门一系统”集约化建设要求，我委信息化以“系统变革、整体重塑”为原则，解构现有信息系统，对数字化整体架构进行优化，完成信息系统国产化改造、信息系统集成整合、信息系统迁移上云、数字化架构优化、安全保障加固工作以及电子政务平台（OA）集成，以全面提升监管服务能力。

本项目建设将对财务监管信息系统、产权管理综合信息系统、省属企业干部人才管理系统、党建信息管理系统、考核分配管理系统、省属企业投资管理系统、国资国企在线监管平台系统等业务系统进行统一国产化适配改造、迁移上云以及数字化架构优化。通过系统国产化适配改造、集成整合和省政务云迁移，构建可持续的数字化服务体系，全面实现系统安全可控、数据互联互通与服务高效便捷，为支撑全省国资国企在线监管与决策提供坚实保障。

一、总体目标

按照“系统整合全面上云、国产化适配全面覆盖、服务能力全面升级，安全保障全面加固”的总体思路，完成省国资委信息系统国产化改造、信息系统集成整合、信息系统迁移上云、数据迁移治理、数字化架构优化及安全保障加固等任务。通过统一技术标准、统一数据规范、统一综合门户、统一安全体系的协同机制，实现系统高效、安全上云，进一步提升监管效能与数字政府建设水平。

二、技术要求

（一）总体要求

1.政策及标准符合性要求

供应商须按照国家和江苏省有关政务信息化项目管理要求、基本建设工程管理规定、财政资金管理要求以及相关网络安全、国产化要求以及统一的技术标准、数据规范与安全规范等实施项目。

2.实用性要求

项目实施过程中，供应商应调研招标人实际使用需求，并结合最新行业政策和业务需求进行系统建设，但总体范围和框架不得偏离项目实施方案和招标文件。

3.统一规范要求

本项目涉及的系统改造须遵守统一的 UI 设计规范、代码编写规范、部署规范、数据规范等要求，如因供应商未按统一规范要求开发和实施导致的返工，由供应商承担一切责任，并无偿按规范整改，否则不予验收。

（二）系统性能要求

1.系统性能指标

总体要求：系统支持从数据层面到业务层面高可用，满足系统可用性；系统易于扩展，

支持海量数据存储，支持业务集群和存储集群，满足高可靠性需求；系统具备充分的数据冗余及数据容错能力；系统具备完善的数据加密和数据传输的安全机制、专业的认证体系和数据访问机制，保障数据安全；确保系统具有高度的安全性，提供安全的登录和访问措施，防止系统被攻击。

应用性能要求：常规网页加载时间不超过 1 秒，简单查询响应时间不超过 2 秒，复杂查询响应时间不超过 5 秒；统计分析类业务一般统计时间不超过 3 秒；复杂统计分析时间不超过 5 秒。

高并发处理能力：系统支持正常 2000 个同时在线用户的性能要求，当 500 个用户并发请求同一个中等复杂度的事务时，响应时间不超过 5 秒。

2. 技术先进性指标

技术成熟度：按照国产化适配目录，选取市场主流、成熟的技术框架。

兼容性：支持与省政务平台、省大数据共享交换平台对接，并预留接口与其他系统（如国务院国资委、设区市国资委、省属企业、司法大数据、省智慧资产监管平台等）可点对点对接。

可扩展性：系统支持在不影响现有功能的情况下扩展新功能。

3. 安全性指标

数据安全：系统确保数据不被未授权访问、篡改或泄露，实现数据加密存储和传输；部分业务系统与外部系统进行数据对接时，确保数据传输与存储安全；数据中台数据上云后确保可用不可见。

系统安全：具备防范常见网络攻击的能力。

访问控制：具备基于角色的访问控制能力。

4. 可靠性指标

系统应提供 7×24 小时的连续运行，平均年故障时间小于 1 天，平均故障修复时间小于 30 分钟。系统具备较强的灾难恢复能力。

5. 用户体验指标

用户满意度：用户对系统易用性、功能性和服务质量的满意度≥99%。

用户界面友好性：界面设计简洁，操作直观，实现主流桌面终验浏览器、移动浏览器适配与适老化适配。

（三）数据迁移治理要求

供应商可以基于现有数据治理软件进行数据迁移与治理，也可自己提供数据迁移工具或治理软件及配套的数据服务。供应商需建立组织架构、流程规范，并配置专职的团队，在招标人指定的系统配套的数据库中按要求开展数据迁移及治理工作，为省国资委数据资源（含历史数据）提供成熟的数据服务。

（四）国产化要求

本项目相关的系统须按照有关要求部署至省政务云安全可靠环境，须支持相关国产化的芯片、操作系统、中间件和数据库等要求，以确保可在省政务云全国产化环境中正常运行。

（五）密码应用要求

围绕国家及江苏省关于政务信息系统在系统规划阶段的密码应用要求，综合考虑系统物理和环境、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、有效的密码应用方案，满足《信息安全技术信息系统密码应用基本要求》三级指标要求和密码应用安全性评估要求。

（六）网络安全要求

1.满足等保测评要求

本项目应按照《信息安全技术网络安全等级保护基本要求》第三级安全要求进行建设。项目建设期和免费质保期内，供应商应按照等保 2.0 标准，配合招标人完成网络安全等级保护测评，并依据专业的第三方测评机构出具的测评结果进行必要的升级完善。

2.满足软件测评要求

本项目建设期内发生的软件升级、修复等代码迭代，均应配合招标人完成软件系统测评，并依据专业的第三方测评机构出具的测评结果进行必要的软件升级完善。

3.满足密码应用安全评估要求

供应商在项目建设期和免费质保期内应及时响应招标人提出的密码应用安全性评估要求，配合完成相应的安全评估，并依据专业的第三方评估机构出具的评估结果开展必要的软件升级、修复。

4.配合完成有关部门的各类安全检查及检测结果处理

供应商在项目建设期和免费质保期内应配合招标人做好有关部门的网络安全检查准备工作，确保通过网络安全检查；对有关部门网络安全检测结果能够及时响应，出具方案并整改。

5.网络信息安全要求

供应商应履行维护网络安全的责任和义务，帮助招标人了解安全隐患并及时部署防御措施，保护网络产品和重要网络系统的安全稳定运行。

供应商应具备信息安全漏洞全局处置能力，协助招标人排查信息系统安全风险，并提出信息安全改进措施。

6.其他要求

（1）严格权限访问控制，用户在经过身份认证后，只能访问其权限范围内的数据，只能进行其权限范围内的操作。

（2）不同的用户具有不同的身份和权限，需要在用户身份真实可信的前提下，提供可信的授权管理服务，保护数据不被非法/越权访问和篡改，要确保数据的机密性和完整性。

（3）对输入有提示，数据有检查，防止数据异常。

（4）系统健壮性强，能处理系统运行过程中出现的各种异常情况，如：人为操作错误、输入非法数据、硬件设备失败等，系统能正确的处理，恰当的回避。

（5）各种数据对接过程中需保护数据不被非法/越权访问。

（6）人工智能技术应用开发过程中，做好敏感数据识别及保护，确保信息安全、意识形态安全。

（七）数据备份要求

项目实施过程中，供应商应建立上云系统的数据备份机制，实现云上数据本地备份，并按招标人要求将关键数据备份至指定位置。

三、功能要求

（一）国产化适配改造和迁移上云

基于省政务云提供的国产化环境，按照国家与江苏省相关工作要求，对省国资委核心业务系统开展国产化改造，实现操作系统、数据库、中间件及应用层的全面国产化，确保系统底层架构自主可控，并完成迁移上云工作，满足省级政务信息系统整合上云的统一部署和安全要求。

1.系统范围

本项目涉及的核心业务子系统包括财务监管信息系统、产权管理综合信息系统、省属企业干部人才管理系统、党建信息管理系统、考核分配管理系统、省属企业投资管理系统、国资国企在线监管平台系统等。

2.国产化适配改造要求

供应商须对省国资委业务系统进行全栈国产化改造，覆盖服务器、操作系统、数据库、中间件、浏览器及关键第三方依赖等软硬件环境。

（1）操作系统替换

供应商须将现有应用服务器操作系统全部替换为国产操作系统，并完成内核参数优化、驱动适配和系统调用替换。

（2）数据库与中间件适配

数据库须由现有 SQLServer/Oracle 等非国产数据库替换为国产数据库，并完成数据结构、索引、存储过程、精度约束等适配与优化。

中间件须由 IIS/Tomcat 等替换为国产中间件，完成配置迁移、JNDI 适配、鉴权加密策略重建。

供应商须确保改造后系统在新数据库和中间件环境下功能完整、性能不低于现有水平，并通过数据迁移验证和压力测试。

（3）应用层改造

供应商须对全部系统代码进行审查和兼容性改造，替换数据库驱动、修改 SQL 语句、

优化前端页面、适配国产浏览器和国密算法。

与报表、全文检索、消息通知等功能相关的接口须重构或适配，确保核心业务功能在国产化环境下完全可用、性能达标。

需替换或重构所有依赖国外商用组件的第三方库和工具。

（4）系统迁移与部署

在完成国产化改造并通过测试后，供应商须将系统统一部署至省政务云互联网区和电子政务外网区（具体根据安全需求部署），并按实际需求实现数据交换和跨网访问。

（5）安全与合规

供应商须按照《网络安全等级保护 2.0》三级及以上标准开展安全加固，采用国密算法（SM2/SM3/SM4）进行数据存储和传输全链路加密。

系统必须具备基于角色的访问控制和统一审计能力，确保敏感数据“可用不可见”，并满足省政务云安全接入要求。

3.迁移上云要求

供应商需完成上述系统从本地物理服务器/虚拟化环境向省政务云平台的迁移部署，构建基于云架构的弹性、可扩展运行环境，摆脱对本地硬件资源的依赖，提升资源利用率与系统可用性；实现系统与省政务云平台的深度适配，包括云服务器、存储、网络、安全等资源的标准化配置，保障系统在云环境下稳定运行，核心业务功能（如数据处理、流程审批、信息交互）响应效率不低于本地环境；依托省政务云平台的安全防护能力与容灾机制，强化系统安全防护水平，实现数据多副本存储与故障快速恢复，满足业务连续性要求，同时降低本地质保成本与硬件投入；打通系统与省政务中台、其他云上业务系统的对接通道，实现资源共享与业务协同，为后续系统整合与数字化转型奠定基础。

（1）硬件资源迁移

1）计算资源

将原本地物理服务器/虚拟化主机承载的应用服务，迁移至省政务云平台的国产架构云服务器，根据系统业务负载需求，配置相应 CPU 核数、内存容量，保障计算资源充足且弹性可调。

2）存储资源

将原本地磁盘、存储阵列中的结构化数据（数据库文件）与非结构化数据（文档、图片、视频等），迁移至省政务云分布式存储或对象存储服务，按数据访问频率与重要性选择存储类型（高性能存储/容量型存储），确保数据存储安全与访问高效。

3）网络资源

梳理原系统网络拓扑（如 VLAN 划分、路由配置、端口映射），在省政务云平台重构网络环境，包括配置私有网络、子网、安全组、弹性公网 IP、负载均衡等网络资源，保障系统内外网访问通畅与网络隔离安全。

（2）软件资源迁移

1）操作系统

将原本地服务器的操作系统替换为省政务云平台支持的国产操作系统，确保与云服务器硬件架构兼容。

2）数据库系统

将原本地数据库，迁移至省政务云平台的国产数据库服务或云原生数据库服务，完成数据库实例创建、数据迁移与参数优化。

3）中间件与工具

将原本地部署的中间件、开发工具、流式软件、版式软件、第三方组件，替换为省政务云平台支持的国产中间件或云原生中间件服务，以及对应的工具，确保软件依赖适配云环境。

4）应用系统

将原本地部署的业务应用（含代码、配置文件、依赖库）迁移至省政务云服务器，完成应用与云环境的适配改造，确保应用正常启动与功能完整。

（3）数据资源迁移

1）结构化数据

包括系统数据库中的业务数据（如用户信息、业务表单、流程记录）、配置数据（如参数设置、权限规则），通过数据迁移工具完成全量迁移与增量同步，保障数据完整性与一致性。

2）非结构化数据

包括业务产生的文档、图片、视频、日志文件等，通过文件同步工具或对象存储接口，批量迁移至省政务云存储服务，建立数据与应用的关联关系，确保迁移后可正常访问。

3）历史数据

对系统历史业务数据（如归档文件、历史记录）进行梳理和去重，确保迁移治理后的数据高可用。

4.指标要求

国产化率：应用系统及配套的服务器操作系统、数据库、中间件国产化替换率100%。

迁移准确率：核心数据迁移准确率100%，实时同步延迟不超过5秒。

安全指标：高危漏洞修复率100%，渗透测试与等保测评均需通过并出具合格报告。

（二）信息系统集成整合

以“系统整合全面上云、国产化适配全面覆盖、服务能力全面升级、安全保障全面加固”为核心导向，锚定省国资委信息系统国产化改造、信息系统集成整合、信息系统迁移上云、数据迁移治理、数字化架构优化及安全保障加固等任务，聚焦用户整合、能力整合、数据整合三大核心维度，通过统一技术标准、数据规范、综合门户与安全体系，破除现有

各个核心业务系统“信息孤岛”问题，实现系统高效安全上云，提升国资国企监管效能，适配数字政府建设要求，为国资委智能化穿透式监管筑牢技术底座。系统集成需求如下：

1.用户整合：构建统一用户体系

（1）用户身份与权限统一

打破各系统独立用户体系壁垒，整合现有分散的用户账号资源，基于省政务中台统一身份认证能力，建立覆盖全系统的统一用户身份库，实现“一人一账号”。按“最小权限”原则，统一规划用户角色与权限矩阵，如“业务人员”“监管员”“系统管理员”等角色，明确各角色在不同系统中的操作权限，避免权限冗余或缺失，解决用户需记忆多套账号密码、频繁切换系统的问题。

（2）登录与访问协同

依托统一综合门户，实现用户“一次登录、全域访问”，用户通过门户完成身份验证后，可直接跳转至各关联系统功能页面，无需重复登录。同步整合用户操作行为日志，统一记录用户在各系统中的登录、业务办理、数据访问等操作，形成完整的用户行为轨迹，为安全审计与用户行为分析提供支撑，提升用户操作便捷性与系统管理效率。

2.能力整合：汇聚共性与业务能力

（1）共性能力复用

梳理各系统共性功能，剥离系统内冗余的共性模块，按需调用省政务中台的身份认证、OFD、OCR、电子签章等共性能力组件，减少重复开发，降低维护成本，确保共性能力的一致性与稳定性。

（2）国产化能力适配

结合国产化改造要求，整合国产化软硬件能力，统一替换各系统非国产化组件，构建统一的国产化技术底座。例如，所有系统均采用国产操作系统、国产数据库、国产中间件，同步整合适配后的共性工具（如国产数据迁移工具、漏洞扫描工具），确保全系统国产化能力覆盖一致，避免因技术栈碎片化导致的适配差异，保障系统在国产化环境下稳定运行。

3.数据整合：实现全域数据贯通

（1）数据标准统一

依据政务数据相关规范，结合省国资委业务特性，制定统一的数据标准体系，涵盖数据元定义、编码规则、格式规范、质量要求等。例如，统一“项目编号”“人员 ID”“企业编号”等核心数据元的字段类型、长度、编码规则，消除不同系统间数据定义差异；建立数据质量监控机制，对数据完整性、准确性、一致性进行实时校验，如企业基本信息元数据必填项校验、跨系统数据关联一致性校验，确保数据质量达标。

（2）数据资源汇聚

省国资委数据中台整合各个核心业务系统的结构化数据与非结构化数据，按业务主题建立数据资源目录，实现数据“一站式”汇聚。同步对接外部数据资源，形成全域数据资

源池，支撑数据“一网共享”。

（三）数字化架构优化及安全保障加固

1.数字化架构优化

省国资委信息系统集成整合上云项目遵循“系统整合全面上云、国产化适配全面覆盖、服务能力全面升级，安全保障全面加固”的总体思路，实现集约化建设。

（1）门户入口

省国资委将建设形成统一门户（含专属门户）入口，外部用户（企业、设区市国资委等）及内部用户（省国资委机关业务相关人员）均通过省国资委综合门户统一访问相关应用。

（2）业务应用

本项目建设将依托现有政务信息系统为支撑能力底座，包括统一的用户、流程、待办、审批等共性服务能力组件，结合各业务应用的个性化需求，对财务监管信息系统、产权管理综合信息系统、省属企业干部人才管理系统、党建信息管理系统、考核分配管理系统、省属企业投资管理系统、国资国企在线监管平台系统进行统一升级改造与迁移整合，同时满足桌面终端浏览器、移动浏览器等不同场景下的视觉呈现需求，从而进一步提升国资国企监管效能与数字政府建设水平。

（3）应用支撑

迁移与改造省国资委现有政务信息系统，提升现有共性服务能力；对接模块则打通与设区市国资委、省属企业等的技术通道，实现监管数据的采集、整理，并经过数据清洗、整合、结构转化等过程，实现应用系统的数据共享、工作协同，提高国资委监管效率与效能。

（4）数据资源

升级改造原始库、标准库，包括内部管理库、企业基本信息库、项目库、产权库、三重一大决策库、财务数据库等在内的数据集市，优化内部大数据运行环境，形成省国资委内部数据资源中心。

（5）基础设施

依托省数字政府的电子政务外网、互联网完成集约高效、资源整合、信息共享、互联互通、安全可靠的信息系统基础运行环境建设。现有机房做数据备份、应急支撑。

（6）标准规范体系

本项目在数字化架构优化过程中，严格遵循国家及省级政务信息化建设的相关政策和技术规范，确保系统建设的合规性、规范性与可扩展性。项目将重点围绕数据分级分类标准的编制与应用，建立统一的数据管理规范，明确数据分级分类的原则、范围与适用对象。

（7）安全保障体系

安全保障体系是针对省国资委政务信息系统环境可能遇到的各种安全威胁和风险，通

过健全信息安全规章制度、加强关键信息基础设施和重要信息系统安全防护、实施网络安全监测预警、制定网络安全应急预案、提高数据安全防护能力等手段，确保基础设施、网络、应用等各项资源的安全、可靠运行。

（8）保障管理体系

通过引入先进成熟的保障管理体系，确保基础设施、网络、数据、应用等各项资源的稳定、高效运行，全面提高国资委信息工作质保质量。依托信息系统工程全方位管理的思想和方法，有效整合管理资源和管理对象，形成规章制度有效、岗位职责清晰、信息传递顺畅、绩效评价规范的管理新格局。

2.软件功能需求

迁移改造后的软件功能不少于原系统软件功能，须满足省国资委政务信息化工作需求。

3.安全保障加固

根据国家网络安全政策法规和技术标准体系的有关要求，落实网络安全等级保护制度，围绕江苏省国资委现有系统安全保护对象的安全保护需求，针对系统重要数据进行分级分类管理，从安全物理环境、安全通信网络、安全区域边界、安全计算环境及安全管理中心等方面考虑防护要求。

（1）安全物理环境

按照等级保护三级标准要求，省政务云部署系统的物理运行环境须遵循计算机场地安全标准，配备相应的安全设施，确保系统连续稳定运行。

（2）安全通信网络

按照安全域划分原则建立隔离保护机制和访问控制策略，杜绝未授权访问。

采用授信机制及加密协议，对省政务云与访问端的数据传输进行加密，避免篡改或窃取，并采用校验与密码技术确保通信过程的机密性和完整性。

充分利用省政务云的密码服务能力，实现用户鉴权认证、数据传输加密保护等功能。

（3）安全区域边界

按照等保三级要求建立安全区域边界防护体系。

（4）设备与计算安全

对关键设备的访问、系统资源控制信息和可执行程序须进行完整性保护，防止篡改。

采用密码技术对设备登录用户进行身份鉴别和远程访问加密，防止口令被窃取或恶意破解。

（5）应用与数据安全

按照《中华人民共和国密码法》和 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》，使用国密算法（SM2、SM3、SM4）实现核心业务数据的存储和传输加密、完整性保护和访问鉴别。

关键业务数据须分级分类管理，敏感数据需全生命周期保护，确保“可用不可见”。

平台须建立统一的身份鉴别、访问控制、日志审计和重要数据灾备机制。

（6）统一安全监控与风险预警

充分使用省政务云提供的入侵防御、漏洞扫描、异常行为识别、日志审计等安全设备及资源，完善安全运营中心（SOC）和集中监控平台。

制定并演练应急响应与灾难恢复预案，支持双活或异地容灾架构，实现分钟级故障切换。