

首都之窗运行管理中心 服务采购合同

合同名称：北京市基于大模型的政务咨询场景建设

第一包：应用软件开发、数据资源建设、

大模型调用和云上其他服务合同

合同编号：京政数合【2025】168 号

委托人（甲方）：首都之窗运行管理中心

受托人（乙方）：首信云技术有限公司

甲方：首都之窗运行管理中心

法定代表人：刘莎

地址：北京市通州区留庄路 5 号院 2 号楼

联系人：赵珣阳

联系电话：18600590808

乙方：首信云技术有限公司

法定代表人：廖伟

地址：北京市通州区台湖镇京通街 9 号 211-2 室

联系人：任晰

联系电话：18600951599

甲方 北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务 项目（以下简称“本项目”）经 北京国际工程咨询有限公司（采购代理机构）以 BIECC-25CG90354/1 号招标文件在国内公开招标。经评标委员会评定乙方为中标人。甲乙双方本着友好合作、平等互利的原则，经双方友好协商，同意按照下面的条款和条件，签署本合同，以资双方共同遵守。

一、合同名词术语定义

1.1 “合同”

系指甲乙双方就本项目达成并签署的协议，包括所有的附表、附件以及下面指出的构成合同的所有文件。双方同意下列文件作为本合同不可分割的组成部分：

- 1、本合同；
- 2、在本合同实施过程中双方共同签署的补充文件；
- 3、乙方递交的全套投标文件及澄清文件；
- 4、招标文件及其变更或澄清文件；
- 5、本项目中标通知书；

甲乙双方同意在出现合同理解上的歧义时，按照以上顺序解释。

1.2 “合同价款”

系指根据本合同规定乙方在正确、全面地履行合同义务后，甲方应支付给乙方的费用。

1.3 “交付物”

系指乙方根据本合同、招标文件的规定须向甲方交付的一切成果物。

二、合同标的

1、甲方同意委托乙方进行 北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务项目 的服务与运营工作。

2、乙方提供的项目服务与运营的内容包括应用软件开发（知识中枢建设、任务调度模块建设、政务咨询智能体建设）、数据资源建设、大模型调用和云上其他服务。通过本项目建设，积极而稳妥地在政务行业落地大模型应用。一是实现用户视角的AI应用场景服务标杆示范，二是实现多元化知识融合利用与运营模式创新，三是实现人工智能应用落地赋能政务服务转型。具体项目服务内容及要求详见附件1。

三、合同期限及进度计划

3.1 合同期限

本项目服务期自合同签订生效之日起 12 个月内完成项目全部服务内容（自合同签订生效之日起 6 个月内完成软件开发相关工作，后续进行不少于 6 个月的试运行工作）。

3.2 进度计划

项目实施周期为自合同签订之日起 12 个月：第一阶段完成项目规划设计与开发（包括需求调研、系统设计、系统开发）；第二阶段完成项目集成及初验；第三阶段开展项目试运行及完成终验，且初验应在合同签订生效之日起 6 个月内完成、试运行工作不少于 6 个月、终验应在服务期结束后进行。

甲方有权根据工作需要，要求乙方调整或加快工作进度，乙方需予以配合。

四、合同价款及支付方式

4.1 合同价款

合同总价款为人民币伍佰壹拾贰万陆仟陆佰伍拾元整（小写：¥5,126,650.00）。该价格包含乙方因履行本合同及招标文件的全部服务内容可能产生的一切费用，包括但不限于税费、各种运营服务费、交通费、劳务费，除此之外，甲方无需再向乙方支付任何费用。

本合同价款包括：应用软件开发费用为人民币贰佰陆拾万元整（小写：¥2,600,000.00

元，含税）；数据资源建设费用为人民币壹佰柒拾陆万元整（小写：¥1,760,000.00 元，含税）；大模型调用费结合测算标准，据实结算，但金额不超过人民币伍拾肆万壹仟壹佰贰拾元整（小写：541,120.00 元，含税），测算标准为：输入单价 0.004 元人民币/千 tokens，输出单价 0.016 元人民币/千 tokens；云上其他服务费用为贰拾贰万伍仟伍佰叁拾元整（小写：¥225,530.00 元，含税，包括：密码服务 106,960.00 元、其他 118,570.00 元）。

4.2 支付方式

本合同的付款方式为：分期付款。

合同签订生效，且项目财政资金拨付到位，甲方在收到乙方提供的发票后 10 个工作日内，甲方向乙方支付 365,443.99 元人民币，大写：叁拾陆万伍仟肆佰肆拾叁元玖角玖分，作为首付款，包括：应用软件开发 184,944.36 元人民币，大写：壹拾捌万肆仟玖佰肆拾肆元叁角陆分；数据资源建设 125,337.21 元人民币，大写：壹拾贰万伍仟叁佰叁拾柒元贰角壹分；大模型调用费 39,321.48 元人民币，大写：叁万玖仟叁佰贰拾壹元肆角捌分；云上其他服务 15,840.94 元人民币，大写：壹万伍仟捌佰肆拾元玖角肆分。

项目终验且项目财政资金拨付到位后，甲方在收到乙方提供的发票后 10 个工作日内，向乙方支付合同金额包括：应用软件开发 2,415,055.64 元人民币，大写：贰佰肆拾壹万伍仟零伍拾伍元陆角肆分；数据资源建设 1,634,662.79 元人民币，大写：壹佰陆拾叁万肆仟陆佰陆拾贰元柒角玖分；云上其他服务 209,689.06 元人民币，大写：贰拾万玖仟陆佰捌拾玖元零陆分。大模型调用费尾款结合测算标准，据实结算，但金额不超过人民币伍拾万壹仟柒佰玖拾捌元伍角贰分（小写：501,798.52 元人民币），如大模型调用费总实际发生金额小于首款（39,321.48 元人民币，大写：叁万玖仟叁佰贰拾壹元肆角捌分），则乙方需退回未实际发生金额。

（本项目使用资金保障证明采购，如财政到位资金金额低于本合同约定的服务费总额，则乙方同意实际结算金额以财政资金到位金额为准，且承诺不向甲方另行主张其他任何费用。）

4.3 乙方指定的收款账户如下：

开户行：中国建设银行股份有限公司北京中关村支行

户名：首信云技术有限公司

账号：11050192360000000776

如乙方收款账户发生变更，乙方应在本合同约定的相关付款期限前【10】日以书面方式

通知甲方，通知应加盖乙方公章。因乙方未及时将通知甲方而产生的一切后果，由乙方自行承担。

4.4 甲方每次付款之前，乙方需提供同等金额的增值税普通发票。乙方拒绝提供发票的，甲方有权拒绝付款且无需承担任何违约责任。

4.5 乙方知悉并确认，甲方付款资金来源为财政性资金，如因财政拨款不足或迟延等非甲方自身原因导致甲方未能按约定付款的，不视为甲方违约，甲方无须承担违约责任。

五、双方权利及义务

5.1 甲方权利及义务

1、项目实施过程中，甲方有权对乙方履行本合同的情况、质量保证情况等进行监督和检查，如发现不符合甲方要求的，有权要求乙方及时整改。

2、甲方指派一名项目负责人，负责本项目的组织管理。甲方如变更项目负责人，应提前 10 个工作日书面通知乙方。

3、甲方应根据乙方提出的要求及时协调业务部门进行必要的沟通和交流。

4、甲方安排乙方人员到甲方现场工作时，应提供乙方人员开展工作所必要的条件，包括但不限于网络环境、工作场所，以保证工作顺利完成。

5、甲方负责组织有关人员在规定的时间内进行项目验收工作。

6、甲方应按照合同约定，及时支付合同款。

5.2 乙方权利及义务

1. 乙方须组织相关专家、技术人员等会同甲方指定人员成立项目组，负责本项目的具体实施工作。

2、乙方应委派 1 名项目经理，并按照招标文件要求进行服务团队配置。乙方不得随意撤换主要技术人员及项目经理等核心人员，如确需更换，必须提前 10 个工作日书面通知甲方，并经甲方同意，同时应做好相关的移交工作。

3、乙方须保证其拥有从事本项目实施工作的资质及实施能力，并根据本合同约定的需求按时、按质完成项目运营的各项工作，为甲方提供可行的技术解决方案，并组织相关项目人员进行实施。

4、乙方在项目验收前，需向甲方提交相应月报、半年报、年报等项目运营的各类文档。

5、乙方应保证所提交的文档与资料的合法性。如甲方被指控侵犯了第三方的所有权、

商业秘密、专利权、版权或其它知识产权等任何权利，乙方必须承担已经发生和可能发生的一切法律责任和相关费用，并赔偿甲方因此产生的一切损失。

6、乙方人员在甲方现场工作期间,应严格遵守甲方的有关规章制度。

7、乙方履行义务不符合本合同、招标文件的要求的，乙方需在甲方指定的时间内改正。

8、乙方应按照招标文件要求提供及时的服务响应，公布服务支持电话，当系统遇到异常（包括但不限于乙方失误、维护不当、被第三方攻击等），无法正常提供服务时，乙方应在 10 分钟内做出响应，通过但不限于电话和现场服务开展故障处理工作。

9、乙方需履行的其他义务以招标文件、采购需求及投标文件承诺的内容为准。

10、乙方应将意识形态工作责任落实到项目全流程，把握正确的政治方向，严守政治纪律、组织纪律、宣传纪律，确保导向正确。

11、乙方在提供服务的过程中，应保证内容来源真实准确，不涉及敏感信息和涉密信息，不存在涉及国家主权、涉及港澳台、涉及领导人的政治性错误，不会造成不良舆情，给甲方造成不良社会影响。否则，甲方有权要求乙方立即采取积极措施消除影响并赔偿由此给甲方造成的损失，并承担相应法律责任。

12、乙方应定期组织党风党纪教育、廉洁警示教育和作风建设教育。把意识形态工作摆在重要位置，坚持意识形态工作与项目服务同步部署。

13、乙方应制定一套科学合理的培训方案。培训的人员类型主要为网站相关业务管理人员、编辑人员、技术运维人员。培训方式以面授和上机实践相结合的方式，应根据甲方指定的不同类型的培训人员，编制相应的培训教材。

六、交付

乙方须提供符合国家规范的网站运营标准，并按照项目管理要求、招标文件和双方约定的时间进行项目运营文档、管理文档等资料的交付。

七、验收

1、项目由甲方组织相关人员组成验收小组负责验收工作。

2、验收内容包括运营工作任务完成情况检查、项目管理检查及项目档案检查。验收指标和成果物交付以招标文件要求为准。

3、乙方应提前 10 个工作日通知甲方并向甲方提交验收申请书，甲方应在 10 个工作日内组织验收工作。

4、验收不合格的，甲乙双方协商一致的情况下可延长验收的期限，延长期以 10 天为限；验收仍不合格的，甲乙双方协商一致的情况下可延长最终验收的期限，延长期以 30 天为限。

5、项目初验后启动试运行，以连续运行 6 个月各项功能能够正常使用，性能达到本合同约定及甲方预期要求为准，组织项目最终验收，在完成项目的移交、培训、文档整理工作后，进入正式运行阶段和售后服务阶段。

八、需求变更

1、在本合同履行过程中，甲方进行需求变更或乙方建议进行需求变更时，均需经双方同意，并采用书面形式进行确认。

2、在双方未就需求变更达成一致之前，乙方应继续履行其义务，视同双方就变更未达成一致。

3、本合同生效后，如果发生以下情况：增加新的运营工作需求，经甲乙双方确认后，可视为重大需求变更。此类变更超出本次项目运营内容，甲乙双方应另行进行协商并签署书面协议。

九、知识产权

1、乙方保证交付的全部设计文件、文档资料、服务成果在中国境内或境外没有且不会侵犯任何第三方的知识产权（包括但不限于版权、商标权、专利权）或专有技术或商业秘密或其他合法权益。乙方保证，如果其提供的设计文件、文档资料、服务成果使用或包含任何第三方的知识产权或专有技术或商业秘密，乙方已经获得权利人的授权。乙方进一步保证使甲方免于因被指控侵权而产生的或与此有关的任何及所有责任，并赔偿甲方由此发生的任何成本、费用和损失，包括但不限于解决争议，甲方因此支出的交通费、律师费、诉讼费等一切合理费用，并保证甲方的正常使用。否则，乙方退还全部合同价款，并赔偿因此给甲方造成的损失。

2、乙方在履行和完成本合同项下工作过程中准备及开发的一切资料，包括但不限于文件、图表、报告、数据、模型和样品，以及其中含有的所有发明和可授版权（包括版权的商业使用权，如：商业推广、纪念品等由版权而带来的延伸产品的开发的资料，为甲方独有的

排他性财产而不受任何限制。甲方有权使用上述资料以履行本项目合同或用于其他目的。该资料应与本项目合同项下其他资料一起，按要求在本项目合同结束或终止的时候，交还给甲方或以甲方认可的方式进行销毁。

十、保密条款

1、保密信息

本合同保密信息特指乙方因履行本合同而知悉的甲方的行政文件、会议纪要、内部信息、内部规范性文件或规章制度、本合同内容及本项目所涉及的全部文件、技术文档、数据以及其他任何甲方尚未对外公开的信息或资料。

2、保密期限

自本合同生效之日起至相关保密信息公开为止。本合同项下的保密义务不因本合同的终止、解除而终止。

3、披露和使用保密信息的限制

乙方应将保密信息的使用限制在乙方及乙方相关工作人员范围内，乙方只可将保密信息用于本合同之目的。乙方须确保其工作人员知悉且同意本条款的内容并确保受其约束。乙方同意，除非按法律法规规定、司法机关或有关监管机构的要求披露外，未经甲方事先书面同意，乙方及乙方工作人员不得向任何第三方披露、转让、复制保密信息或以其他方式谋取任何利益，也不以任何形式为本合同目的以外的目的使用保密信息。

4、违约责任

乙方或乙方工作人员违反保密义务的，乙方需按照本合同总金额的 20%向甲方支付违约金，并赔偿由此给甲方造成的损失。

5、保密信息的返还或销毁

本合同解除或终止时，如甲方要求乙方返还或销毁任何依本合同而提供的保密信息及其复印件，乙方应在甲方要求的时间内返还或销毁。

十一、不可抗力

1、本条所称不可抗力是指无法预见、无法避免、无法克服的致使本协议全部或部分义务不能履行或不能如期履行的客观情况，包括但不限于自然灾害如水灾、台风、地震等，以及社会事件如战争、动乱、罢工、政府行为或法律规定等；

2、本协议项下任何一方对于因不可抗力致使本协议不能履行或不能全部履行而给对方造成的任何损失不承担赔偿责任；

3、如果发生不可抗力事件，则受影响的一方应采取积极有效的措施以减少因本协议不能履行或不能全部履行而给对方造成的损失，并应在不可抗力事件发生后及时通知对方，并在 7 个工作日内出具官方证明文件；

4、因不可抗力影响因素消失以后，双方应协商是否继续履行本协议，如不可抗力因素致本协议已无法履行，双方应终止本协议。

十二、合同变更、转让及终止

12.1 合同变更

1、本合同一经生效，非经甲乙双方书面同意，任何一方以任意方式对合同条款的增减及其他变更均无约束力。

2、对合同的任何修改和变更，任何一方需提前 5 个工作日向另一方发出书面通知。

12.2 合同转让

非经甲乙双方书面同意，任何一方无权转让本合同及该合同约定的全部或部分权利、义务。

12.3 合同终止

1、合同自然终止：甲乙双方全部履行合同及相关附件约定的义务后，本合同自然终止。

2、违约合同终止：若合同一方有足够证据证明合同另一方未在规定时间内履行本合同项下规定义务，可向对方提出书面违约通知，提出终止部分或全部合同，合同中未终止的部分应继续履行。

3、破产合同终止：如合同一方破产或有证据证明其无清偿能力，另一方可在任何时候以书面形式通知对方，提出终止合同而不给对方补偿，或要求资产保全防止损失扩大。本合

同的终止将不影响甲方、乙方采取或将要采取的任何行动或补救措施的权利。

十三、违约责任

1、甲乙双方任何一方不履行合同义务或者履行合同义务不符合约定的，均视为违约，需赔偿由此给对方造成的全部损失。

2、乙方应按照双方约定的时间完成本合同项下的各项运行维护服务，乙方迟延提供前述服务的，每延迟一日需按照本合同总金额的千分之【五】按日支付违约金，超过【10】日仍未完成交付或通过验收或提供相关服务的，乙方需按照本合同总金额的 20%向甲方支付违约金，如违约金不足以弥补损失的，乙方需继续赔偿，同时甲方保留解除本合同的权利，甲方解除合同的，乙方需退还已收取但未完成或未经甲方验收通过部分的费用并按照本条款约定支付违约金、赔偿金。

3、乙方交付的成果经两次以上（包含两次）验收仍然不合格的，经甲方合理宽限后仍不能验收合格的，乙方需按照本合同总金额的 20%向甲方支付违约金，如违约金不足以弥补损失的，乙方需继续赔偿，同时甲方保留解除本合同的权利，甲方解除合同的，乙方需退还已收取但未完成或未经甲方验收通过部分的费用并按照本条款约定支付违约金、赔偿金。

4、乙方违反本合同、招标文件、投标文件的其他任一任何承诺、保证、义务或责任的，均视为违约，乙方应就违约行为按照本合同总金额的 20%向甲方支付违约金，如违约金不足以弥补损失的，乙方需继续赔偿，同时甲方保留解除本合同的权利，甲方解除合同的，乙方需退还已收取但未完成或未经甲方验收通过部分的费用并按照本条款约定支付违约金、赔偿金。

5、如由于乙方原因甲方采取司法途径维护其合法权益的，乙方还应赔偿甲方因此产生的合理支出，包括但不限于律师费、诉讼费、保险费、公告费、保全费等。

6、如乙方存在对甲方应付未付款项的，包括但不限于赔偿金、补偿金、违约金等，甲方有权从应付乙方款项中直接扣除，且不因此承担任何违约责任，不足部分仍由乙方另行补足。

十四、法律适用及争议解决

1、本合同按中华人民共和国法律解释。

2、甲、乙双方在合同履行过程中发生的一切争议，均应通过双方友好协商解决；协商不成的，任何一方均可向甲方住所地有管辖权的人民法院提起诉讼。

十五、通知

1、任何根据本合同要求发出的通知或者其他通讯（包括但不限于司法机关、政府部门、有权机构的通知、函件以及沟通文件）应以中文书写，并经专人、挂号信、电子邮件或传真送至本合同记载的地址。

2、任何一方的通讯地址或联系方式如发生变动，应立即书面通知其他方，因未及时通知而造成的损失由通讯地址或联系方式变动方自行承担。

3、本合同记载的地址的适用范围包括非诉阶段和争议进入仲裁、民事诉讼程序后的一审、二审、再审和执行程序；因一方提供或者确认的送达地址不准确、送达地址变更后未及时依程序告知对方和法院、一方或指定的接收人拒绝签收等原因，导致法律文书未能被实际接收的，邮寄送达的，以文书退回之日视为送达之日；直接送达的，送达人当场在送达回证上记明情况之日视为送达之日。

十六、合同生效及其他

1、本合同书一式叁份，甲方一份，乙方贰份，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。

2、合同未尽事宜，双方本着相互信任和谅解的原则，友好协商解决并签订补充协议。

3、本合同的附件与本合同具有同等法律效力，是本合同不可分割的一部分。本合同的附件包括：

附件 1. 项目服务内容及要求

附件 2. 项目实施计划与安排

附件 3. 项目服务团队配置

附件 4. 项目经费明细表

附件 5. 安全及保密协议

附件 6. 网络意识形态安全协议

附件 7. 廉政责任书



法定代表人(或授权代表)签字:

签订日期: 2025 年 10 月 12 日

签订地点: 北京市通州区



法定代表人(或授权代表)签字:

附件 1. 项目服务内容及要求

北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务项目建设内容包括应用软件开发（知识中枢建设、任务调度模块建设、政务咨询智能体建设）、数据资源建设、大模型调用和云上其他服务。

1. 知识中枢建设

1.1 外部素材库

通过对接各单位知识库等系统，定时抓取汇总到外部素材库中，对这些知识进行知识清洗、图像识别、文本解析等工作将知识内容解析成可识别的文字后再进行知识内容进行重复检测、冲突检测，并可提交采用流程。包括：

1.1.1 单位政务知识库定制化开发对接

通过接口对接实现定期调用各单位知识系统提供的标准知识，保证知识及时获取和更新。

1.1.2 知识清洗

开发数据清洗模块，对知识中 HTML 格式符号等格式问题，将清洗的后的知识存储入库。

1.1.3 文本解析

对知识的附件，格式包括 doc、docx、PDF 等，开发文本解析模块，将文件中内容解析成系统可识别的文字。

1.1.4 OCR 识别

对知识段落内包含的图片、链接，开发自动获取并存储图片数据功能，利用开源 OCR 模型开发 OCR 识别功能，提取图片内容并还原至原文中。

1.1.5 政务文件消歧管理

通过对接获取的增量数据与已采用入库的数据自动进行知识内容重复及冲突比对并展示结果及内容。

1.1.6 知识采用

对经过处理后的知识由用户进行采用至知识底库模块。

1.1.7 知识供给接口开发

开发提供对外知识供给标准接口，实现对外供给知识服务。

1.2 知识底库

汇聚外部素材库中已采用的知识数据，可以对知识数据进行管理维护并可对知识进行文本切片、QA 知识智能生成等操作，处理之后的文本切片和 QA 知识分别存储于知识管理库相应的模块中并具备冲突检测功能还能对其原始知识进行溯源。包括：

1.2.1 相关政务文本管理

对外部素材库中采用的各类知识数据进行编辑、查询、删除等常规操作，另外开发创建知识功能。

1.2.2 文本智能切片

开发文本内容智能切片，保证段落内容完整可用。

1.2.3 QA 智能生成

利用大模型以文章切片和提示词作为输入，智能生成一批与文章片段内容相关的 QA 知识，并将这些知识存储到知识库中。

1.2.4 QA 知识冲突检测

对增量入库的 QA 知识与知识库中旧知识进行比对，发现新旧知识差距，辅助运维人员开展知识处理。

1.2.5 政务问答对管理

支持增删改 QA 类知识，支持搜索查询，支持批量上传、删除、批量生效/失效。

1.2.6 知识溯源

将政务问答对逐个选择关联相关政策文件，建立用户自定义上传的问答对与政策文件之间的关联关系。

1.3 知识管理

针对单位业务专家录入的标准问答、内部知识等数据进行管理，支持知识编辑、存储、溯源等配置操作，同时具备维护风控拒答模板、政务词库、敏感词库、知识数的功能，还可对热门知识进行管理。包括：

1.3.1 QA 库

将知识底库中由大模型生成的 QA、用户自定义上传的 QA 汇总管理，包括对知识的编辑、删除、批量上线、批量下线等功能。

1.3.2 切片库

将知识底库中文本智能切片汇总管理，包括对切片的编辑、删除、批量上线、批量下线等功能。

1.3.3 风控拒答模版库

管理安全风控应答口径知识、非政务范围等的拒答模版知识。

1.3.4 政务词库

将涉及较专业的业务专有词汇、百姓常用词汇、业务词汇等词汇一一对应，并进行配置管理。

1.3.5 敏感词库

提供敏感词增删改模块，用于管理风控链路中敏感词检测环节。

1.3.6 知识树

为实现大模型多轮问答，需对业务逻辑配置，建立知识引导树。搭建知识树体系及层级节点并构建节点提示词、挂接相关 QA 知识等用于引导用户提问。

1.3.7 热门知识管理

对关注度高的热门问题及高频知识进行定期管理，支持录入编辑热门问题和答案，用户点击问题后，直接给出标准答案。

1.4 知识回流管理

针对测评数据和对话数据建立回流配套功能管理，业务专家可执行测评任务辅助提升问答水平，同时对回流数据进行分析，进而查漏补缺，提高知识利用效率。包括：

1.4.1 问答效果专家评测

1.4.1.1 专家 AI 评测

为业务专家提供问答测评窗口，供业务专家自由提问测评、打分及备注功能。

1.4.1.2 评测字典管理

提供测评字典后台修改选项的功能，由管理人员编辑维护。

1.4.1.3 自定义配置管理

针对每一个评测项目，开放知识树配置开关、敏感过滤开关、子知识库选择功能，支持灵活配置。

1.4.1.4 构建测评集

构建自定义创建测评问答数据集，支持对测评集进行增删改操作，可支持批量数据导入和删除。

1.4.1.5 知识 AI 搜索

构建智能快速搜问的功能，利用大模型能力进行搜索，展示库中相关问答知识，点击知识标题可查看详情及相似度，及模型生成结果。

1.4.2 回流数据管理

1.4.2.1 小模型部署微调

部署分类小模型，按业务需要及相关训练数据利用微调工具对模型进行微调，微调有效性模型、清晰度模型、业务分类模型等实现初步对回流数据的标注。

1.4.2.2 小模型数据处理

按照不同的标签规则，利用微调后的多个小模型进行数据自动打标功能。

1.4.2.3 回流数据管理

支持用户对回流数据进行人工打标签处理，支持回流数据的查看功能。

1.4.2.4 知识补全管理

构建知识补全的任务流程，将有问题的回流数据提交流转至委办局用户处理，对缺失知识进行补充细化后，由运营人员进行采用入库处理。

1.5 政务咨询支撑组件

构建可用性高且可有效规避潜在使用风险，通过采取安全风控措施加以管理，防控大模型生成内容涉及隐私数据、敏感内容等易引发负面舆情或违反规定情况的问答咨询服务。包括：

1.5.1 政务咨询界面配置

1.5.1.1 政务咨询界面开发

设计开发大模型政务咨询服务页面，基于统一规范要求，设计开发清晰的提问输入框、热门问题推荐、答案溯源内容展示等功能。

1.5.1.2 地图服务插件设计与开发

根据用户问题提供相关咨询地点的地图渲染展示功能。

1.5.1.3 用户登录页面 UI 设计及开发

设计开发政务咨询用户登陆界面。

1.5.1.4 政务咨询页面前端开发 H5 适配

为政务咨询界面做 H5 适配，确保桌面端与移动端风格一致，界面功能操作设置统一。

1.5.1.5 问答溯源关联配置

根据问答召回的参考依据，匹配对应的知识文件并提取 URL 展示在前端界面，支持点击查看文件内容。

1.5.1.6 安全回退开发配置

支持灵活配置安全回退功能，支持由大模型问答切换至依据标准问答库输出标准答案。

1.5.2 安全风控

1.5.2.1 安全风控链路管理

开发安全风控模块，构建敏感词识别、正则匹配、风控语义模型识别等环节，对风险问题过滤，同时设置了各级敏感数据回答话术模板。

1.5.2.1.1 敏感词识别

依据知识管理中敏感词库实时更新，配置敏感词回答模版，对敏感词进行甄别。

1.5.2.1.2 特定词正则匹配

通过正则匹配实现安全风险过滤，积累特定词组搭配，配置正则匹配回答模版。

1.5.2.1.3 风控语义模型

使用分类模型实现安全风险过滤，设计多分类标签及配置多分类标签下的回答模版。

1.5.2.2 标准 QA 过滤库

为用户提供标准 QA 库增删改的管理模块，当用户提问与标准 QA 达到阈值时直接带出库中已有标准答案。

1.5.2.3 兜底答复配置

开发设置回答阈值，若用户问题低于阈值需带出回答模版。

1.6 综合配置及问答调测管理

通过自然对话交互的形式进行问答效果进行调测，并支持相关配置管理。包含：

1.6.1 综合配置管理

在一个模块中构建集成知识树、热门问题、提示词管理、风控模板等功能，供用户快速配置各项数据。

1.6.2 问答调测管理

构建大问答测试模块,应用综合配置管理模块的各项配置,且在配置项正式发布生效前,用于测试、效果调优等工作。

1.6.3 提示词管理

构建大模型提示词管理功能,通过可视化界面调整提示词并技术接口配对响应模型。

1.7 融合库建设

为更充分地挖掘利用知识,提高知识的多元性,通过知识融合消除孤岛,加强不同业务领域间的知识服务。包括:

1.7.1 多知识库聚合

构建用户自定义选择多个知识库中相关的业务知识并重新组成新的知识库功能。

1.7.2 融合分类目录管理

构建多维度的知识分类及目录管理功能,支持按知识形式、知识属性、知识标签等多维度二次分级分类管理。

1.7.3 融合知识标签管理

支持用户对融合知识条目添加自定义标签,实现融合目录中实现多维度的标签化管理。

1.7.4 融合多维度检索

允许用户根据不同维度(如知识形式、知识属性、业务分类等)进行知识数据的智能检索。

2. 任务调度模块建设

基于大模型智能体能力及流程编排应用技术,构建大模型智能调度模块功能,支持任务规划调度、多智能体协作、对话式创建应用等功能;构建单一入口对接多个业务领域的咨询服务,支持多个业务领域的意图识别、意图分发,实现如公积金问答智能体、交管问答智能体等政务智能体的调度。包括:

2.1 调度任务拆解

开发大模型智能体任务拆解功能,将复杂任务拆解成更小的子任务,分析用户问题所属类型,调用不同专业智能体进行回答。

2.2 调度智能体构建

开发创建调度智能体,由用户以自然语言方式描述需求,自动完成调度智能体创建,并基于配置界面完成选择需要调度的政务咨询智能体、知识库等。

2.3 智能体及组件管理

支持对接内部或外部多个业务类型的政务咨询智能体,提供功能类型的组件(如:地图查询组件等)管理,包括各个智能体的 API、所挂接知识库等。

3. 政务咨询智能体建设

政务咨询智能体覆盖试点单位部门业务领域,借助大模型语义理解、自主学习和智能推理等能力,支持用户提问政务信息提取、政务咨询多轮引导、政务知识数据存储及检索管理、政务咨询答案生成、问答智能体插件调用、接口调用等,促进提升政务咨询服务水平。

3.1 用户提问政务信息提取

用户提问政务信息提取能够支持精准提取用户输入的短语、问题以及文本中包含的语义信息，智能提取文本中包含的实体、关系、问题、事项描述等多维度信息。包括：

3.1.1 问题类型提取功能

提取用户输入的问题中的问题类型，包括咨询事项主题、意图及诉求等问题类型，准确感知用户的提问内容，进行匹配回答。

3.1.2 业务情形提取功能

提取用户输入问题内容中的业务情形，如公积金提取、交管办事地图查询等，根据不同的情形进行匹配回答。

3.1.3 模糊条件澄清功能

当用户输入问题表述模糊、不明确时，通过系统指令提示词及小样本事例等方式，以提问的形式对用户模糊的意图进行澄清问答，确保每一次咨询都能得到有效处理和响应。

3.1.4 确认条件提取功能

根据用户输入的问题信息，匹配知识节点，根据所处情形的条件进行判断来进行匹配回答。

3.1.5 用户问题改写功能

将用户问题根据问题类型、业务情形、条件进行改写，用户问题的可读性。

3.2 政务咨询多轮引导

政务咨询多轮引导包括知识树定义不同业务路径，基于预先配置好的分层级业务以及交互逻辑，支持面对用户不明确的问题，进行总结并追问多轮引导，向用户发送针对性的引导问题，让用户通过多轮聊天的方式，逐步缩小问题范围、明确关键信息，另外要根据用户在一个会话下的历史问题通过大模型能力总结改写新问题，共同完成多轮引导功能。包含：

3.2.1 上下文意图继承功能

开发基于策略结合大模型能力的多轮对话记忆与继承功能，提升问答的连贯性和回答质量。

3.2.2 上下文意图切换功能

开发上下文意图切换功能，发现用户的询问点发生的变化，从而检索更合理的知识对问题进行回答。

3.2.3 知识树服务及接口

构建知识树功能服务，将知识树作为政务咨询后台服务能力的一个环节，此功能将用于理解用户问题澄清和反问环节。

3.3 政务知识数据存储及检索管理

政务咨询知识检索支持根据外部知识中枢提供的政策文件、办事指南、标准问答对以及其他个性化政务知识等数据进行数据清洗、结构化和知识嵌入入库，构建一个后台知识数据库，将不同形态的知识分别存储，同时构建知识向量库，将知识进行索引及向量化。在用户提到与数据库相关问题或答案相关的信息时，引用政务知识库检索库进行回答。包括：

3.3.1 文本嵌入模块

开发微调文本嵌入模型，用于将知识转向量并存储至向量空间数据库中。

3.3.2 知识数据向量库构建

构建多种知识数据向量库存储处理后的向量数据库,以支持大模型在政务咨询中的检索和推理。

3.3.3 文件类知识检索

检索文本类知识向量库,当用户检索政策细节信息时,大模型引用该知识库作出回答。

3.3.4 表格类知识检索

检索表格类知识向量库,支持大模型在相关询问中进行高效检索和精准回答。

3.3.5 问答对类知识检索

检索问答对类知识向量库,在用户提到与问答对中问题或答案相关的信息时,大模型引用问答对类检索进行回答。

3.4 政务咨询答案生成

检索完成后,系统会依据匹配度对检索到的知识切片进行智能排序,最终将相关、最有价值的切片内容给模型参考,将检索到的相关片段与原始问题合并,形成更丰富的上下文信息,调用大模型总结并生成答案回复用户。包括:

3.4.1 政务文件问答

根据政务文件和政务文件知识向量库的内容,调用大模型总结并为用户问题生成答案内容。

3.4.2 表格类知识问答

根据表格类知识库和表格向量库,调用大模型总结并为用户问题生成答案内容。

3.4.3 QA 类知识问答

根据 QA 问答对库和如常见问题等内容,调用大模型总结并为用户问题生成答案内容。

3.4.4 知识来源关联

大模型在引用检索结果时,在推送回答的同时,对来源进行引用展示。

3.5 问答智能体组件调用功能

利用大模型理解用户问题,运用指令自主调用智能体组件功能,包括调用知识库或外部应用系统 API 回答用户问题。

3.6 大模型问答应用功能开发

根据不同单位的业务需求及安全风控要求,分别开发各单位大模型问答应用相关功能接口,供前台应用调用。

4. 大模型调用

4.1 大模型调用(政务咨询智能体)

通过公有云调用大模型服务支撑政务咨询智能体应用,通过调用模型 API 服务以 token 计费方式提供服务,经估算本项目涉及的政务咨询智能体总咨询量每年不低于 100 万次。

4.2 大模型调用(知识中枢)

知识中枢相关功能建设需调用大模型能力来完成知识治理工作,如基于大模型知识检索、知识消歧管理冲突比对、智能生成 QA 问答对,通过调用模型 API 服务以 token 计费方式提供服务,经估算本项目涉及的知识治理相关数据量每月约为不少于 1000 个文件,每个文件

汉字量约为 2000 字。

4.3 大模型的选择

乙方本项目所使用的大模型应从已完成备案的大模型中选用来源可信的大模型，乙方应提出适用本项目大模型应用选型方案。

4.4 大模型调用费的结算方式

通过调用模型 API 服务以 token 计费方式提供服务，本项目周期结束时按照实际模型调用量乘以单价进行费用据实结算，并以大模型调用费分项价款金额为上限。

5. 数据资源建设

5.1 大模型工程化链路维护

5.1.1 应用场景链路维护

大模型应用场景工程落地涉及工作链路搭建、知识梳理与业务逻辑设计、RAG 检索增强及持续优化的复杂过程，需综合考虑多方面模块功能配置，确保安全与性能。

5.1.1.1 问答场景安全风险链路维护

提供安全风险控制及话术模板回复链路维护，收集风险内容，定期微调风险判断链路，提升监控拦截准确度，并保障话术模板回复链路持续有效，维护不少于 10 次并形成《安全风险链路维护清单》。

5.1.1.2 RAG 检索增强链路维护

RAG 检索增强链路设计维护工作主要涵盖数据获取与预处理、索引构建以及检索与生成部分。人工持续维护并优化检索增强链路，确保最相关的结果排在前面，维护不少于 10 次并形成《RAG 检索增强链路维护清单》。

5.1.1.3 政务地图智能调用链路维护

结合用户体验及政务地图应用系统资源，针对用户问询办事地点，优化实现回复地理位置渲染，维护不少于 10 次并形成《政务地图智能调用体验监测清单》。

5.1.2 大模型问答场景效果优化

5.1.2.1 知识冲突及消歧检测维护

基于大模型语义理解能力所开展的知识比对与冲突歧义结果，进行处理维护，确保检测的准确性，维护不少于 10 次。

5.1.2.2 知识数据优化

聚焦于知识分块后的知识粒度管理与持续优化，包括改进文本切分方法，根据政务知识数据，辅助训练更适合中文特性和政务数据的切片工具，优化不少于 10 次。

5.1.2.3 检索模型微调

用微调的方法对模型进行改进，包括优化排序、召回结果，从而提高检索的准确性和相关性，微调不少于 10 次。

5.2 高质量数据集运营管理

大模型政务咨询的应用效果离不开准确可靠的语料数据和高质量的知识数据供给，相关资源过程涉及风险防控训练样例、业务逻辑路径数据、效果评测数据等，需综合管理并长期持续地更新优化。

5.2.1 训练与测评数据集运营

大模型政务咨询应用效果离不开准确可靠的语料支撑和高质量的知识数据供给，相关资源运维过程涉及风险防控训练样例、业务逻辑路径数据、效果评测数据等，需综合管理并长期持续地更新优化。

5.2.1.1 风控模型训练数据集运营

收集风控及敏感词句相关的数据形成训练数据集，对相关数据进行标注，定期进行模型调优。数据集运营不少于 500 条。

5.2.1.2 回流数据标注模型训练数据集运营

对真实用户问答回流数据进行不同维度打标签并形成相关数据集，支撑训练分类模型等工具，数据集运营不少于 5000 条。

5.2.1.3 业务问答效果评测数据集运营

收集整理业务专家评测数据并完善标注问答数据作为训练集，检测大模型在业务知识方面回答应用效果，数据集运营不少于 6000 条。

5.2.1.4 安全效果测评数据集运营

持续构建安全测试数据集，辅助测评大模型在生成对话过程中是否存在不符合法律法规、社会秩序等情况，数据集运营不少于 1000 条。

5.2.2 知识数据质量管理

5.2.2.1 外部数据采用

评估外部数据的准确性、完整性和有效性，针对可用的外部数据进行集成和初步数据处理，筛选处理不少于 30000 条。

5.2.2.2 多形态知识标准化处理

知识库中知识在入库前和入库后分别进行增量数据冲突检测和全量数据冲突检测，人工辅助以下任务优化，标准化处理不少于 2000 条。

5.2.2.3 人工消歧确认及编辑运营

对已完成规范化的知识数据进行逐行的精细化识别治理，包括每行的数据内容规范、缺失数据处理、重复数据处理等，入库不少于 1000 条。

5.2.2.5 缺失知识补充

知识覆盖度不高的领域知识库需要寻找并补充数据源，人工分析额外数据的质量、相关性和安全性，补充不少于 1000 条。

5.2.2.6 知识切片及 QA 生成确认

针对政策文件、政策解读、操作详解等长文本类知识进行切片处理，切片结果生成问答对入库，不少于 1000 条。

5.2.3 知识运营管理

5.2.3.1 内部知识溯源关联

对已入库的各类知识进行溯源关联，追踪知识的来源和生成过程并对知识进行版本管理，关联不少于 1200 条。

5.2.3.2 补充内部知识溯源关联来源

针对无法溯源的知识，需要在外部数据中寻找相有关联的来源信息，并补充进知识库中，补充不少于 1000 条。

5.2.3.3 风控模版库梳理维护

将不同类型的风险管理模板进行分类，如舆情风险、误导风险、操作风险等，为每个模板设定合适的风控规则，包含触发条件、阈值等，维护不少于 150 条。

5.2.3.4 知识树构建初始化

人工梳理 10 个智能体主要业务的知识点，确保涵盖足够的主题领域，将知识点按照主题、子领域进行分类，构建知识树的层级结构，构建不少于 10 个。

5.2.3.5 设计知识树层级关联

设计每一轮多轮对话的逻辑和常用的多轮问答场景，定义用户提出问题后的分支路径，澄清用户的真实意图，设计关联不少于 1000 条。

5.2.3.6 知识树更新维护

根据实际的问答流程和知识点的使用频率，需要人工定期调整知识树的层次结构。不少于 280 个节点。

5.2.3.7 优化知识树分支和节点信息

根据业务需求或用户反馈，引入新的知识点或设计新的业务主体知识树，人工确认业务主体知识树的窗口期，不少于 1000 次。

5.2.3.8 知识组合汇聚维护

根据知识类别或业务场景等需要，进行知识组合汇聚管理，及时更新知识条目并调整失效组合知识，做好关联维护，不少于 1000 条。

5.2.3.9 核心词库维护

支持政务领域核心业务词管理，实现增、删、改、查等功能维护，包括政务专有词、敏感词库等，不少于 1000 条。

5.2.3.10 提示词维护

针对通用共性场景、单独个性场景或不同业务领域能够提供相应的提示词模板配置，不少于 10 套模板。

5.2.4 服务场景质量监测

5.2.4.1 服务场景单轮问答质量监测

定期对 10 家试点单位的大模型政务咨询开展业务、风险、安全等方面的单轮对话测评，并监测分析记录结果，按月处理不少于 3000 条记录并形成检测记录。

5.2.4.2 服务场景多轮问答质量监测

定期对开展 10 家试点单位业务、风险、安全等方面的多轮对话测评，并分别记录测评结果，按月处理不少于 3000 条记录并形成检测记录。

5.2.4.3 测评回流数据标注

针对大模型测评数据结果进行分析打标，包括标注模型优化的责任单位，确认问题原因并测试模型优化后的效果，不少于 1000 条记录并形成问题清单。

5.2.4.4 问答效果统计分析

围绕线上用户问答量、对话轮次等实际咨询情况，以及点踩点赞等服务反馈情况进行统计，按月形成统计分析报告。

5.2.4.5 舆情监测预警分析

定期监测与测评问答对话潜在风险，跟踪大模型生成回复友好性，针对敏感、违规、易引发舆情或影响安全管理的内容进行分析洞察及处理，按月形成监测预警报告。

5.2.4.6 服务场景日常监测分析

针对不同领域及服务场景渠道的问答量、知识调用情况等进行统计，监测分析不同服务场景知识及热门问答知识构建应用效果，按月形成日常监测报告。

6. 政务云上其他相关服务

提供符合采购方需求的北京市市级政务云（服务云）上其他相关服务，详细服务内容及需求如下：

序号	服务类	服务描述	服务期 (年月)	计量 单位	数量
一	基础软件支撑服务				
1-1	商用操作系统套餐	国产 Linux 套餐：国产 Linux 操作系统服务租用、安装及维护。	6	台	18
1-2	国产商用应用中间件套	国产商用应用中间件租用、安装及维护	6	台	13
1-3	商用数据库套餐	国产商用数据库租用、安装及维护（至少支持 3 种国产数据库）	6	台	2
二	安全服务				

2-1	云端抗 DDOS 服务	云端抗 DDOS 服务	6	站点	1
2-2	云端 APT 防护服务	云端 APT 防护服务	6	台	1
2-3	主机杀毒服务	主机杀毒服务	0.5	台	15
2-4	主机防护	主机防护	0.5	台	15
2-5	主机安全加固	主机安全加固	0.5	台	15
2-6	网页防篡改服务	网页防篡改服务	6	监控点	5
三	安全检测、监测、 审计服务				
3-1	主机漏洞扫描	主机漏洞扫描	0.5	台	15
3-2	主机日志分析	主机日志分析	0.5	台	15
3-3	数据库审计服务	数据库审计服务	0.5	台	2
四	密码服务				
4-1	强身份认证服务	面向业务系统，通过云服务的模式提供基于数字证书的强身份认证技术支持，本服务支持 SM2 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，本服务可以配合 USBKey 证书 PC 端以及业务服务之间的强身份认证。	6	月	1
4-2	签名验证服务	面向业务系统，通过云的模式提供签名验证服务，支持 SM2/SM3/SM4 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，基于数字签名技术对业务系统中关键数据和操作进行签名及验签。	6	月	1
4-3	加解密服务	面向业务系统，通过云平台的模式提供加解密技术支持，支持 SM2/SM3/SM4 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，实现对系统中重要数据的机密性保护。	6	月	1
4-4	SSL 安全服务	面向业务系统，通过云的模式提供 SSL 安全服务，支持 SM2/SM3/SM4 算法，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而	6	月	2

		确保通信时的身份鉴别、通信数据的机密性和完整性。			
4-5	远程运维接入服务（国密）	面向运维人员，提供国密远程运维的接入服务（国密），支持 SM2 算法证书登录。	6	月	4
4-6	设备证书	标识系统映射 IP，与 SSL 安全服务搭配使用，构建 HTTPS 通道。	6	月	4
4-7	个人数字证书（含介质）	标识系统终端用户数和运维人员的网上身份，并配置智能密码钥匙，对登录用户进行身份鉴别。	6	月	10
4-8	国密浏览器	为系统运维人员和超级管理员终端配置国密浏览器，构建国密传输通道。	5	个	5

7. 性能要求

（1）处理能力及响应速度

涉及业务系统功能的，在网络稳定的环境下，简单操作平均响应时间小于 1 秒，一般查询平均响应时间小于 3 秒。

涉及大模型服务的，在网络稳定的环境下，简单问题提交至答案生成首字平均响应时间小于 5 秒，系统应确保单个简单问题请求的完整返回结果时间不超过 20 秒，以满足实时处理的需求。

（2）可扩展性和可维护性

平台应具有良好的兼容性，易于扩展、修改模块、增加新的功能以及服务发布、注册、流程配置；允许共性组件对应接口功能进行扩展。网站应具有良好的兼容性，易于扩展、修改、增加新的栏目及内容。

（3）易用性和容错性

平台应具备人机界面友好、服务使用快捷、功能操作简单方便，简洁明了。具备良好的容错性，具备检错、纠错功能，保证数据的正确性、一致性和完整性。

8. 安全要求

本项目应用软件开发部分需按照国家安全等级保护三级目标进行建设。在项目建设过程，按照国家有关信息系统安全等级保护的基本要求，全面实现信息系统的物理安全、网络安全、主机安全、应用安全、数据安全，使本项目相关系统达到国家安全等级保护三级要求。本项目要求满足国产化需求，支持国产化主流操作系统、数据库、中间件。

本项目涉及提供生成式人工智能服务的，应当按照国家有关规定开展安全评估，并按照《互联网信息服务算法推荐管理规定》履行算法备案相关手续。

9. 培训要求

供应商应制定一套科学合理的培训方案。培训的人员类型主要为网站相关业务管理人员、编辑人员、技术运维人员。培训方式以面授和上机实践相结合的方式，应根据不同类型的培训人员，编制相应的培训教材。

10. 验收要求

甲方依据招标文件、投标文件、合同条款，及甲方制定的信息化项目验收的规定与标准进行验收，验收小组的组成包括甲方业务部门和技术部门的相关人员，或聘请相关专家。

1. 验收指标

(1) 本项目需按照等保三级标准建设。

(2) 完成知识中枢建设、任务调度模块建设、政务咨询智能体建设，以及大模型工程化链路维护、高质量政务数据资源建设并提供大模型调用服务保障。

(3) 服务团队具备完善可靠的系统备份和恢复机制和信息安全应急预案和安全应急演练方案。

2. 成果物提交

提交成果物应包括但不限于以下交付物，并作为甲方无形资产：

(1) 项目文档：项目计划、实施方案、系统需求说明书、详细设计说明书、数据库设计说明书、质量保证计划、系统运行和维护所必需的原始资料、程序维护手册、用户操作手册、培训文档、信息安全应急预案和安全应急演练方案文档。

(2) 软件开发部分的程序源代码、系统安装程序（提供电子文档）。

11. 项目关键需求指标

(1) 政务知识录入管理 ≥ 100000 个。

(2) 政务知识治理消歧 ≥ 10 次。

(3) 问答知识树配置管理 ≥ 14 个。

(4) 接口配置与联调 ≥ 20 个。

(5) 提供政务咨询智能体应用服务 ≥ 10 个。

(6) 政务咨询问答测评 ≥ 10 次。

(7) 会话回流分析 ≥ 10 次。

(8) 稳定运行率 $\geq 98\%$ 。

(9) 故障响应率及排除率 $\geq 99\%$ 。

(10) 故障响应修复时间 ≤ 4 小时。

(11) 大模型知识运营服务保障时间 ≥ 6 个月。

(12) 用户满意度 $\geq 90\%$ 。

附件 2. 项目实施计划与安排

北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务项目完成期自合同签订生效之日 12 个月内完成项目全部服务内容，项目初验后启动试运行，以连续运行 6 个月各项功能能够正常使用，性能达到合同预期为准，组织项目最终验收，完成项目的移交、培训、文档整理工作，进入正式运行阶段和售后服务阶段。项目实施周期为 12 月：第一阶段完成项目规划设计与开发（包括需求调研、系统设计、系统开发）；第二阶段完成项目集成及初验；第三阶段开展项目试运行及完成终验，且初验应在合同签订生效之日起 6 个月内完成、试运行工作不少于 6 个月、终验应在合同签订之日起 12 个月内完成。

序号	工作内容		执行周期
1	项目规划设计与开发阶段	(1) 项目需求调研 (2) 项目团队建立 (3) 系统设计 (4) 系统开发	自项目合同签订后 4 个月内完成。
2	系统集成及初验	(1) 集成测试 (2) 初步验收	自项目合同签订后 6 个月内完成。
3	项目试运行及终验	项目试运行	项目初验后至项目终验前。（不少于 6 个月）
		最终验收	项目服务期结束后进行。
4	项目归档	项目、资产、技术归档	项目终验后。

附件 3. 项目服务团队配置

序号	姓名	专业	本项目中担任岗位	资质/备注
1	任晰	管理科学与工程	项目总监	信息系统项目管理师（高级） 核心人员
2	徐嘉琪	电子工程	项目经理	核心人员
3	邢博	情报学	系统架构师	系统架构师（高级）、系统分析师（高级）
4	董晔	贸易经济	知识架构师	系统规划与管理师（高级） 核心人员
5	范云飞	计算机科学与技术	系统分析师	系统分析师（高级）
6	苏佩瑶	计算机科学与技术	数据工程师	数据库系统工程师
7	陈俞玢	软件工程	需求分析师	核心人员
8	吴小博	计算机科学与技术	知识数据分析师	ITIL
9	徐劭	自动化	知识数据分析师	人工智能应用工程师（高级）
10	王宁	软件工程	知识数据分析师	核心人员
11	王一	电子科学与技术	算法工程师	信息系统项目管理师（高级） 核心人员
12	王迪	电子信息工程	软件开发工程师	信息系统项目管理师（高级）
13	詹晓巍	计算机科学与技术	软件开发工程师	无
14	余宗旺	软件工程	软件开发工程师	无
15	王颖	交互设计、自动化	美工设计师	无
16	翁洁伟	管理科学与工程	实施工程师	信息系统项目管理师（高级）

序号	姓名	专业	本项目中担任岗位	资质/备注
17	李艳玲	计算机科学与技术	测试工程师	软件高级测评师
18	符纯嘉	商务管理	知识体验优化师	核心人员
19	刘璐	城市规划	知识体验优化师	无
20	王腾	数字媒体技术	知识体验优化师	核心人员
21	齐英杰	计算机科学与技术	知识合规工程师	无
24	万国权	网络工程	云计算工程师	VCP 认证证书、IBM CTSS 证书、ORACLE 证书、ITIL 证书
25	张颖	计算机软件	质量工程师	ISO 20000 内审员、国际培训师、ISO9000 内审员、CMMI

附件 4. 项目经费明细表

序号	分项名称	合价（元）	备注/说明
1	应用软件开发	¥2,600,000.00	应用软件开发含知识中枢建设、任务调度模块建设和政务咨询智能体建设。
2	数据资源建设	¥1,760,000.00	数据资源建设含大模型工程链路维护 and 高质量数据集运营管理。
3	大模型调用	¥541,120.00	大模型调用含大模型调用（政务咨询智能体）和大模型调用（知识中枢），本项目综合考虑市场公有大模型计费单价，最终按照输入单价 0.004 元人民币/千 tokens，输出单价 0.016 元人民币/千 tokens 报价。
4	密码服务	¥106,960.00	云上密码服务。
5	云扩展	¥118,570.00	云上扩展服务含基础软件支撑服务、安全服务等。
总计		¥5,126,650.00	

附件 5. 安全及保密协议

安全及保密协议

鉴于乙方正在向甲方提供北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务，为做好甲乙双方的安全和保密工作，经友好协商签订本协议。

一、乙方应加强对乙方服务人员的约束，并定期进行安全和保密教育。

二、乙方及乙方服务人员须遵守以下规定：

1. 认真学习相关安全、保密制度，并在工作中严格遵守。

2. 对因工作需要所掌握的国家秘密、工作秘密和敏感信息负有保密责任，严格遵守国家保密法律、法规、规章和甲方的保密制度，不得擅自扩大知悉范围，确保国家秘密、工作秘密的安全。

3. 严格遵守国家秘密在制作、收发与传递、使用、复制、保存、销毁等方面的保密规章制度。

4. 保障或参加甲方会议时不带无关人员进入会议场所，严格会议文件和会议内容的保密管理。

5. 不得擅自将涉及甲方网络和信息系统以及工作秘密的内容写入自己的著作、稿件中，不在自媒体及朋友圈发布。

6. 不在私人交往、私人通信中涉及国家秘密和工作秘密。不在公共场所谈论国家秘密。不在无保密保障的电话、传真、计算机和网络上传递、传输国家秘密，不带无关人员进入甲方保密要害部门、部位。

7. 不得擅自离职，经单位批准离职时，严格履行保守秘密的义务。

8. 自觉接受保密教育、信息安全教育，自觉接受保密监督、检查。

9. 未经允许，非工作时间不得在甲方办公场所擅自驻留、留宿。

10. 不得私自将与工作无关人员带入甲方办公场所。

11. 在甲方办公场所不得私自搭建网络，不得访问与业务无关的非法网站。

12. 除应当遵守《中华人民共和国网络安全法》、《信息安全技术个人信息安全规范》、

《中华人民共和国数据安全法》等现行法律法规外，还应遵守甲方内部数据安全方面的有关管理规定。

13. 妥善保管数据信息，不得私自复制、泄露或遗失，且未经甲方批准，不得以任何形式或任何方式将数据信息或其中任何部分，泄露给任何第三方。

三、本协议自甲乙双方法定代表人或授权代表签字并加盖公章之日起生效。有效期为自本合同生效之日起至相关保密信息公开为止。

四、本协议一式 3 份，甲方执 1 份，乙方执 2 份，每份具有同等法律效力。

甲方：首都之窗运行管理中心

(盖章)

法定代表人或授权代表

(签字)

乙方：首信云技术有限公司

(盖章)

法定代表人或授权代表

(签字):

签订日期：2025年10月22日

签订日期：2025年10月22日

附件 6. 网络意识形态安全协议

网络意识形态安全协议

鉴于乙方正在向甲方提供北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务，为全面落实《网络信息内容生态治理规定》的要求，进一步加强意识形态工作，甲乙双方友好协商，达成本补充协议如下：

一、工作责任

1. 甲方应不定期的对乙方项目团队落实意识形态工作责任的情况进行监督、检查，如发现乙方的意识形态工作落实不到位，或存在不符合甲方要求的情形，甲方有权向乙方提出整改意见。

2. 乙方要严格遵守《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国网络安全法》及其他国家有关法律、法规和行政规章制度。

3. 乙方要严格遵守《非经营性互联网信息服务备案管理办法》《网络信息内容生态治理规定》等国家相关部门管理规定。

4. 乙方保证不得利用网络危害国家安全、泄露国家秘密，不侵犯国家、社会、集体利益和第三方的合法权益，不从事违法犯罪活动。

5. 乙方不得利用甲方信息系统制作、复制、发布、传播含有下列内容的信息：

- 1) 反对宪法所确定的基本原则的；
- 2) 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- 3) 损害国家荣誉和利益的；
- 4) 歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；
- 5) 宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；
- 6) 煽动民族仇恨、民族歧视，破坏民族团结的；
- 7) 破坏国家宗教政策，宣扬邪教和封建迷信的；
- 8) 散布谣言，扰乱经济秩序和社会秩序的；
- 9) 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

- 10) 侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；
 - 11) 法律、行政法规禁止的其他内容。
6. 乙方应当采取措施，防范和抵制制作、复制、发布含有下列内容的不良信息：
- 1) 使用夸张标题，内容与标题严重不符的；
 - 2) 炒作绯闻、丑闻、劣迹等的；
 - 3) 不当评述自然灾害、重大事故等灾难的；
 - 4) 带有性暗示、性挑逗等易使人产生性联想的；
 - 5) 展现血腥、惊悚、残忍等致人身心不适的；
 - 6) 煽动人群歧视、地域歧视等的；
 - 7) 宣扬低俗、庸俗、媚俗内容的；
- 8) 可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的；
- 9) 其他对网络生态造成不良影响的；
 - 10) 其他危害计算机信息安全的。
7. 甲方有权对乙方执行本协议和相关规定情况进行检查，乙方应予以配合，对检查中发现的问题应积极整改。
8. 乙方如违反本协议规定，应承担相应的法律责任，给甲方造成损失的，应赔偿给甲方造成的一切直接损失，并负有为甲方消除不良影响，恢复名誉的义务。

二、争议的解决

因履行本补充协议产生争议的，甲乙双方应通过友好协商的方式予以解决。协商不成，双方同意依法向甲方所在地有管辖权的人民法院提起诉讼。

三、其他

1. 本协议自甲乙双方法定代表人或授权代表签字并加盖公章之日起生效，至项目合同终止时终止。

2. 本协议一式 3 份，甲方执 1 份，乙方执 2 份，每份具有同等法律效力。

甲方：首都之窗运行管理中心（盖章）

乙方：首信云技术有限公司（盖章）

法定代表人或授权代表（签字）：

法定代表人或授权代表（签字）：

签订日期：2025年10月22日

签订日期：2025年10月22日

附件 7. 廉政责任书

廉政责任书

鉴于乙方正在向甲方提供北京市基于大模型的政务咨询场景建设第一包：应用软件开发、数据资源建设、大模型调用和云上其他服务（以下简称本项目），为做好本项目服务过程中的党风廉政建设，经甲乙双方友好协商，订立廉政责任书如下：

第一条 甲乙双方的权利和义务

- （一）严格遵守党和国家有关法律法规及北京市的有关规定。
- （二）严格履行合同中规定的各项义务。
- （三）双方的业务活动坚持公开、公正、诚信、透明的原则（法律认定的商业秘密和合同文件另有规定的除外），不得损害国家和集体利益，违反国家及北京市各项规章制度。
- （四）建立健全廉政制度，开展廉政教育，公布举报电话，监督并认真查处违法违纪行为。
- （五）发现对方在业务活动中有违反廉政规定的行为，有及时提醒对方纠正的权利和义务。
- （六）发现对方存在严重违反本责任书的行为，有建议给予处理并要求告知处理结果和向其上级有关部门举报的权利。

第二条 甲方的义务

- （一）甲方及其工作人员不得索要或接受乙方的礼金、有价证券和贵重物品，不得在乙方报销任何应由甲方或个人支付的费用等。
- （二）甲方工作人员不得参加乙方安排的超标准宴请和娱乐活动；不得接受乙方提供的通讯工具、交通工具和高档办公用品等。
- （三）甲方及其工作人员不得要求或者接受乙方为其住房装修、婚丧嫁娶、配偶子女的工作安排以及出国出境、旅游提供方便等。

第三条 乙方义务

(一) 乙方及其工作人员不得以任何理由向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品。

(二) 乙方及其工作人员不得以任何名义为甲方及其工作人员报销应由甲方单位或个人支付的任何费用。

(三) 乙方及其工作人员不得以任何理由安排甲方工作人员参加超标准宴请及娱乐活动。

(四) 乙方及其工作人员不得为甲方单位和个人购置或提供通讯工具、交通工具和高档办公用品等。

第四条 违约责任

(一) 甲方及其工作人员违反本责任书第一、二条，依据有关规定给予党纪、政纪或组织处理，调离其工作岗位；涉嫌犯罪的，移交司法机关追究刑事责任；给乙方单位造成经济损失的，应予以赔偿。

(二) 乙方及其工作人员违反本责任书第一、三条，依据有关规定，给予党纪、政纪或组织处理；给甲方单位造成经济损失的，应予以赔偿；情节严重的，甲方可以单方终止与乙方的协议，并且禁止乙方在三年内参与甲方组织的项目投标(如有)。

第五条 本责任书有效期为乙方签署之日起至该项目验收合格之日止。

第六条 本责任书作为北京市基于大模型的政务咨询场景建设 第一包:应用软件开发、数据资源建设、大模型调用和云上其他服务项目合同的附件，与项目合同具有同等的法律效力。

甲方：首都之窗运行管理中心

(盖章)

法定代表人或授权代表

(签字):

乙方：首信云技术有限公司

(盖章)

法定代表人或授权代表

(签字):

签订日期：2025年10月22日

签订日期：2025年10月22日