合同登记编号：

技 术 开 发 合 同

项目名称：OCR 大模型智能识别系统项目

委托人（甲方）： **教育部留学服务中心**

研究开发人（乙方）：**讯飞智元信息科技有限公司**

签订地点： 北京市海淀区北四环西路 56 号

教育部留学服务中心

签订日期： 2026 年 9 月 30 日

依据《中华人民共和国民法典》的规定，合同双方就 OCR 大模型智能识别系统项目的技术开发，经协商一致，签订本合同。

一、标的技术的内容、范围及要求

本项目围绕教育部留学服务中心数智化转型与核心业务数据底座建设需求，依托 OCR 大模型与大语言模型技术，开展智能识别系统开发建设。主要完成但不限于以下开发业务和维护业务:

1. OCR 大模型智能识别系统功能开发建设，包括但不限于智能识别引擎建设、多渠道接入与预处理能力建设、系统架构与 AI 算力保障、系统安全与开发运维保障等。

2. 根据《 OCR 大模型智能识别系统 需求任务书》（详见附件 1），完成 OCR 大模型智能识别系统的系统分析、系统设计、程序设计、软件开发、系统测试、系统上线试运行、系统验收;

3. 乙方开发系统须满足本合同网络安全、数据安全、个人信息保护全部要求，符合国家网络安全等级保护相关规定;

4. 乙方在甲方需要时(如需在中心内网环境进行开发调优和测试等场景时)，派 1 人或多人到达甲方现场进行驻场开发工作;

5. 乙方为甲方提供系统使用培训并为甲方业务经办人员提供本项目相关应用软件技术培训;

6. 乙方提供甲方试运行现场的紧急处理支持;

7. 自项目终验合格之日起，乙方应为项目提供为期一年的免费维护和升级，必要时须提供到达现场的紧急处理支持。在运维期内发现所开发的软件质量缺陷的，乙方应当负责返工或者采取补救措施。如因甲方使用、保管不当引起的问题，乙方在合理需求范围内应提供运维服务，甲方可向乙方支付不超过市场合理价格的运维费用，经双方协商确认后签订补充协议。

二、应达到的技术指标和参数

1. 乙方所交付的技术成果必须是自行开发的，无毒、洁净的，开发行为以及技术成果内容等保证不违反法律、法规及相关政策规定，不侵犯第三方合法权益。因乙方提供的软件产品或乙方开发过程中所涉及的包括侵犯第三方知识产权在内的一切原因给甲方或其他第三方造成任何损失的，乙方应无条件进行全额赔

偿。如涉相关处罚，乙方应当自行承担。

2. 乙方根据其调研了解的用户方需求，完成OCR大模型智能识别系统需求分析。

3. 乙方完成《OCR 大模型智能识别系统项目 需求规格说明书》的编写，会同甲方共同确认以该《OCR大模型智能识别系统项目 需求规格说明书》作为本合同系统开发及验收的依据。

4. 乙方应按照本合同规定之项目建设时间要求，按时按质完成《OCR大模型智能识别系统项目 需求规格说明书》上规定的系统软件开发内容及系统软件环境的安装、调试、开通运行。

5. 系统日志须保留不少于180天，满足审计与追溯要求。

6. 乙方负责向甲方提供所有开发文档和使用手册及其他相关文档。包括但不限于:

《OCR大模型智能识别系统项目 实施方案》

《OCR大模型智能识别系统项目 需求规格说明书》

《OCR大模型智能识别系统项目 概要设计说明书》

《OCR大模型智能识别系统项目 详细设计说明书》

《OCR大模型智能识别系统项目 数据库设计说明书》

《OCR大模型智能识别系统项目 测试方案及测试报告》

《OCR大模型智能识别系统项目 安装部署方案》

《OCR大模型智能识别系统项目 系统运维手册》

《OCR大模型智能识别系统项目 培训方案及培训教材》

《OCR大模型智能识别系统项目 用户使用手册》

《OCR大模型智能识别系统项目 试运行报告》

《OCR大模型智能识别系统项目 总结报告》

《OCR大模型智能识别系统项目 代码开发规范说明书》

《OCR大模型智能识别系统项目 系统安全自查报告》

7. 若乙方为产品代理商，乙方需保证此项目中涉及产品、人员、服务均为原厂产品、人员、服务。乙方在项目执行期间，若因不可抗因素无法继续完成系统建设，需由原厂继续完成项目。乙方在提供的一年免费运维期限内，需提供原

厂运维服务。

三、项目建设时间要求

整个项目开发建设包括 OCR 大模型智能识别系统的用户需求调研及系统分析、系统设计、程序设计、软件开发、系统测试、系统上线试运行、系统验收。

项目开发自合同签订之日起开始实施。202【7】年【2】月起系统主要功能上线试运行。试运行稳定后，甲方进行系统验收。

四、研究开发经费、报酬及其支付或结算方式

甲方根据协议执行进度采取分段方式支付给乙方，所有费用以人民币为结算单位，以银行转账方式结算。

1. 本项目研究开发经费￥1,783,000.00 元（人民币壹佰柒拾捌万叁仟元整）。

2. 支付方式：甲方根据协议执行进度采取分段方式支付给乙方，所有费用以人民币为结算单位，以银行转账方式支付。

2.1 本合同签订后，在乙方向甲方开具符合要求的正式发票后 10 个工作日内，甲方向乙方支付第一笔款项（合同款总额的 60%），即￥1,069,800.00 元（人民币壹佰零陆万玖仟捌佰元整）；

2.2 系统部署上线后，在乙方向甲方开具符合要求的正式发票后 10 个工作日内，甲方向乙方支付第二笔款项（合同款总额的 30%），即￥ 534,900.00 元（人民币伍拾叁万肆仟玖佰元整）。

2.3 系统验收合格且乙方已按合同约定向甲方移交完整源码、技术文档及全部数据成果后，在乙方向甲方开具符合要求的正式发票后 10 个工作日内，甲方向乙方支付第三笔款项（合同款总额的 10%），即￥178,300.00 元（人民币壹拾柒万捌仟叁佰元整）。

五、履行的期限、地点和方式

1. 本合同在北京履行。

2. 本合同自甲乙双方盖章并经法定代表人或授权代表签字之日起生效，项目建设周期不超过一年。本合同于项目验收合格且一年免费运维期满后终止。

3. 本合同的履行方式：乙方负责项目软件开发，并以计算机程序代码进行安装部署，提交给甲方使用，乙方负责项目软件的维修和升级。

六、技术情报和资料的保密

1. 乙方应遵守国家保密法律法规及甲方相关信息安全管理规定、要求，保密信息包括但不限于：甲方提供的业务数据、技术资料、经营信息；乙方在开发过程中接触到的甲方非公开信息；系统开发过程中所获得的技术、资料、个人信息、数据以及本项目产生的源代码、设计文档等。

2. 乙方应采取不低于对其自身秘密所采取的保护措施（且不低于合理的保护程度）对保密信息进行保密，不得向任何第三方披露，亦不得用于本合同以外的目的。乙方应确保其参与人员在签署专项保密协议后，方可接触项目实施工作。保密义务自合同签订之日起生效，且不因本合同的解除、终止或无效而失效，直至相关信息进入公有领域。

七、技术协作和技术指导的内容

甲方协助乙方完善系统的功能需求分析，在试运行阶段协助乙方工程师在甲方的环境中开展工作。

八、项目组成员要求

乙方保证在合同履行期内，本项目实际投入的人员均为乙方公司正式员工，甲方有权要求乙方提供相应证明，若不符合要求或乙方不配合提供，甲方有权单方终止或解除本合同，并要求乙方退回甲方已支付的全部合同款并承担违约责任。

乙方应组建专业、高效且具备丰富经验的项目团队，团队成员需分工明确、职责清晰；指派一名具有十年及以上软件开发工作经验的员工作为项目负责人全程参与本项目的实施工作。项目组成员原则上不得更换，若必须更换的，须提前15 日以书面形式报甲方同意。继任项目人员须继续履行合同约定的职责，做好工作交接，保证项目正常进行。更换的人员须具备同等或高于原人员的资质或资历。未经甲方同意，乙方不得擅自更换项目组成员，擅自更换的，乙方构成违约，应当自甲方发出违约通知之日起 15 日内向甲方支付违约金 50000 元/人/次。因擅自更换人员给项目推进造成影响的，乙方应当根据甲方要求再次调整，且甲方保留单方解除本合同的权利。

九、技术成果的归属和分享

甲方拥有 OCR 大模型智能识别系统 的全部知识产权，包括但不限于全部源代码(含完整注释)、数据库结构及字典、接口文档、第三方授权许可文件、部署脚本及环境配置文件、技术文档、软件著作权等，乙方须向甲方移交上述完整资

料。知识产权及相关资料、数据移交完成并经甲方验收确认(包括源代码可编译性的验证)是甲方支付合同尾款的前提条件之一。未经甲方书面同意，乙方不得将本系统及程序源码转让给第三方。本项目中所有数据、资料的全部权利均归甲方所有，未经甲方同意，乙方不得将相关数据、资料等内容用于本协议以外的其他用途，且乙方不享有对上述数据的任何权利。

十、数据权属与安全

1. 本项目研究开发过程中产生的所有原始数据、中间数据、最终产出数据、衍生数据以及利用研究开发经费购置的设备、器材、资料等全部产权均归甲方(教育部留学服务中心）所有。

2. 乙方在开发及运维过程中接触到的甲方业务数据、技术资料、经营信息及其所有权(如有)、持有权、使用权、经营权、收益权及处置权等全部完整权利均属于甲方。未经甲方书面授权，乙方不享有任何数据权利，乙方不得对数据进行备份、下载、复制、传播或用于本合同以外的任何目的。

3. 乙方应建立严格的数据安全管理制度，采取必要的技术手段确保数据在采集、传输、存储、处理等环节的安全，防止数据泄露、篡改或丢失。本合同因服务期限届满、解除、终止，或乙方发生解散、破产等情形而终止的，乙方处理甲方数据的合法性基础即告丧失，必须立即停止使用并按甲方要求将全部数据及其所有副本予以返还或彻底销毁(包括物理介质归还及电子数据不可恢复擦除)，不得以任何形式留存。乙方不得将甲方数据用于债务清偿、破产清算、资产抵质押或任何其他与本合同无关之用途，确保甲方数据资产与乙方一般财产完全隔离。数据销毁完成后，乙方须向甲方出具由其法定代表人签字并加盖公章的书面销毁证明。（甲方如有另行书面许可的，根据甲方另行书面许可要求及范围使用或处理）。

4. 系统涉及个人信息采集时，必须设置用户同意环节，明确信息使用范围与期限，留存同意记录。

十一、代码开发安全与规范约束

1. 乙方须严格遵循国家信息安全等级保护相关要求、软件工程国家标准及甲方认可的代码开发规范开展全部开发工作，确保代码结构清晰、注释完整、可读性强、易于维护。

2. 乙方开发所用编程语言、框架、中间件、数据库等须使用官方稳定版本，禁止使用存在已知高危漏洞的开源组件、第三方库或非法插件。

3. 智能检索类功能须保证结果真实、准确、可溯源，不得虚构、伪造、篡改；若出现虚假，乙方须在24小时内更正并提交溯源报告。

4. 代码编写须遵循：

(1) 统一命名规范、编码格式规范；

(2) 模块化、低耦合、高内聚设计；

(3) 关键业务逻辑与敏感操作留存可追溯日志；

(4) 禁止硬编码密码、密钥、Token、证书等敏感信息。

5. 乙方在提交验收前，须完成代码安全扫描、渗透测试、漏洞自查，形成可验证的测试记录。

6. 若甲方或第三方检测出高危漏洞，乙方须24小时内响应、48小时内完成修复，并重新提交检测。

7. 因代码不规范、存在安全漏洞导致验收不通过的，按本合同第十四条违约责任执行。

十二、验收的标准和方式

1. 乙方研究开发所完成的技术成果，达到了本合同第二条所列技术指标，且乙方已按第十一条要求完成安全自查并提交全部合格文档，乙方已在甲方指定服务器完成系统部署、数据迁移及关联配置，并向甲方移交完整源代码及文档后，应向甲方提交书面验收申请。甲方在收到乙方完整验收申请材料后，按《OCR大模型智能识别系统项目 需求规格说明书》标准，采用现场调试运行组织验收，验收应包含对数据完整性、系统在甲方环境下的运行稳定性进行测试。由甲方出具加盖公章的技术项目验收证明。任何数据或文档的缺失均视为未完成开发任务，甲方有权拒绝进入验收程序。

2. 验收不合格的，甲方应书面通知乙方不合格事项，乙方应在甲方指定的期限内（原则上不超过5个工作日）完成整改，并重新提交验收申请。

3. 若乙方连续两次验收不合格，或在合理期限内未完成整改，甲方有权单方解除本合同，并依据第十四条相关约定追究乙方违约责任。

十三、风险责任的承担

1. 由于不可抗力因素导致的工作中断，受不可抗力影响的一方就因不可抗力导致的履行不能部分不承担责任，但应及时书面通知对方。不可抗力包括但不限于自然灾害、政府行政命令、国家政策调整、上级主管部门管理要求等不能预见、不能克服且不能避免的客观因素。待条件恢复后，由双方协商并书面确定合同变更内容。

2. 因不可抗力导致合同提前终止的，双方互不承担违约责任。对于合同终止前乙方已完成并经甲方书面确认合格的工作成果，甲方应根据该部分成果对应的合同价款比例向乙方支付费用；若甲方已支付款项超出该部分费用，乙方应在合同终止后【15】个工作日内予以退还，具体结算比例由双方根据项目实际进度协商确定，协商不成的，可共同委托第三方进行评估。

3. 在履行本合同的过程中，非因不可抗力导致研究开发部分或全部失败所造成的损失，风险责任由乙方全部承担。

十四、违约责任

违反本合同约定，违约方应按照《中华人民共和国民法典》的有关条款以及本合同的规定承担违约责任。

1. 逾期违约：若乙方未按约定期限提交验收申请并完成环境部署，乙方应向甲方支付违约金，违约金按照每拖延一天支付本合同总金额的千分之一计算。若延期超过 1 个月，甲方有权单方面解除本合同，自甲方发出解除通知之日起本合同解除，乙方应当于合同解除之日起 1 个月内退还甲方已经支付的合同款项，并支付合同总额 30%的违约金。

2. 验收违约：若项目提交验收后因乙方原因未能通过，乙方应限期整改。整改期间每逾期一日，应支付合同总额千分之一的违约金。若经两次整改仍未通过，或整改累计逾期超过【15】日的，视为根本违约，应支付合同总额 30%的违约金。甲方有权视情况单方解除合同，乙方须返还全部已付款项，并另行支付合同总额 30%的违约金。

3. 数据移交违约：若乙方违反数据、技术成果移交（第九条、第十条）的约定，应向甲方支付合同总额 10%的违约金。若乙方擅自留存、使用、对外转让、许可或以其他方式超越授权范围处理相关数据(包括但不限于利用数据进行模型训练、商业分析、向关联方共享等)，视为严重违约，应向甲方支付合同总额 30%

的惩罚性违约金；若前述行为给甲方造成实际损失(包括但不限于公关危机、行政处罚、第三方索赔等支出)超过违约金金额的，乙方应就全部实际损失承担全额赔偿责任。由此导致项目无法通过验收或投入使用的，甲方有权视情况单方解除合同，并要求乙方退还全部已付款项，并承担甲方因系统迁移、数据恢复等产生的全部合理费用。

4. 安全与规范违约：若乙方违反代码开发安全与规范(第十一条)约定的，存在代码不规范、安全漏洞未整改、未提交安全自查文档等情形，导致验收不合格或影响系统安全运行的，甲方有权要求限期整改；整改后仍不合格的，甲方有权视情况单方解除合同，乙方须返还已支付款项，并支付合同总额 15%的违约金。

5. 人员违约：乙方违反第八条项目组成员要求约定的，按 50000 元/人/次支付违约金，且甲方保留单方解除权。

6. 转包/分包违约：乙方擅自将本项目的全部或部分转让、委托给其他第三方的，甲方有权解除本合同，乙方应立即返还甲方已支付的所有费用，并向甲方支付合同总金额 30%的违约金。

7. 甲方违约：甲方违反本合同第四条约定，应承担以下违约责任：应向乙方支付相应的违约金，违约金按照每拖延一天支付合同约定金额的万分之一计算。

8. 其他：除上述条款外，任何一方违反本协议约定给对方造成损失的，违约方应当就守约方的实际损失承担赔偿责任。

十五、合同的解除与终止

除本合同第十四条违约责任约定外，任何一方如欲单方解除本合同，需提前 20 个工作日书面通知另一方，并说明解除本合同的正当理由，本合同解除事宜需由双方另行协商后签署书面解除协议。

十六、解决合同纠纷的方式

因本合同引起的或与本合同有关的任何争议，双方当事人和解或调解不成，可采取仲裁程序解决。双方同意由北京仲裁委员会按照其仲裁规则进行仲裁。仲裁裁决是终局的，对双方均具有约束力。

十七、其他

1. 本合同一式肆（4）份，双方各执贰（2）份，具有同等法律效力。

2. 任何一方根据本合同发出的通知或其他通信，应以书面形式（包括电子邮

件、快递或专人送达）发送至对方在本合同签署页列明的联系人及地址。通知自送达之日起生效。双方确认签署页所列联系人、电话、地址、电子邮箱为有效联系方式，任一信息变更应提前5个工作日书面通知对方，否则视为未变更。以快递方式发送的，投递后第三日视为送达；以电子邮件发送的，发送成功即视为送达（以系统回执为准）。

3. 本合同附件《OCR 大模型智能识别系统 需求任务书》和《OCR 大模型智能识别系统 数据安全和保密协议》为本合同重要组成部分，与本合同具有同等法律效力。

（以下无正文）

（本页无正文，为OCR大模型智能识别系统项目《技术开发合同》的签署页）

委托人（甲方）	名称(或姓名)	教育部留学服务中心 (签 章)			技术合同专用章 或 单位公章
	法定代表人	李智 (签 章)			
	委托代理人	王梁鹏 (签 章)			
	联系(经办)人	\ (签 章)			
	住所 (通讯地址)	北京市海淀区北四环西路56号辉煌时代大厦	邮政编码	100086	2026年9月30日
	电话	62677915	传真	\	
	开户银行	\			
	帐号	\			
研究开发人（乙方）	名称(或姓名)	讯飞智元信息科技有限公司			技术合同专用章 或 单位公章
	法定代表人	张友国（签 章）			
	委托代理人	（签 章）			
	联系(经办)人	（签 章）			
	住 所 (通讯地址)	安徽省合肥市高新区云飞路66号天源迪科1号楼5-8层	邮政编码	230001	2026年9月30日
	电话	0551-65309171	传真		
	开户银行	招商银行合肥分行三孝口支行			
	帐号	551902934710201			

附件 1

OCR 大模型智能识别系统

需 求 任 务 书

教育部留学服务中心

2026 年 5 月 25 日

目录

1. 背景介绍.....55
2. 核心需求分析.....55
    2.1. 证件识别范围及提取要素.....55
    2.2. 用户端图像智能识别业务需求.....58
        2.2.1. 多渠道图像接入与预处理需求.....58
        2.2.2. 结构化内容提取与智能语义解析需求.....59
        2.2.3. 识别结果交互与质量保障需求.....180
        2.2.4. 双引擎协同与知识库整合需求.....61
    2.3. 大模型应用技术架构与算力需求.....62
        2.3.1. 大模型应用技术架构设计.....62
        2.3.2. AI 算力与弹性扩展需求.....62
    2.4. 系统安全性需求.....64
    2.5. 授权管理需求.....64
    2.6. 个人信息与隐私保护.....65
    2.7. 运维期需求.....65
    2.8. 其他需求.....66
3. 实施计划.....66
    3.1. 项目开发周期.....66
    3.2. 开发人员需求.....67
4. 风险评估与应对策略.....68
    4.1. OCR 识别准确率风险.....68
    4.2. 数据安全与隐私风险.....69
    4.3. 技术融合风险.....69
    4.4. 运营与维护风险.....70
    4.5. 业务衔接风险.....70
5. 结论.....71

1. 背景介绍

本需求书旨在明确拟建设的 OCR 大模型智能识别系统各项需求。该项目通过构建基于 OCR 大模型的基础图像内容挖掘能力，实现多渠道图像材料的高精度文本提取与结构化输出，为后续留学相关业务系统提供高质量的数据底座。

用户可通过 PC 端、小程序端、APP 端等多渠道上传留学相关材料图像（如身份证、护照、港澳通行证、各国签证等），图像经预处理与矫正引擎进行标准化处理后，由 OCR 大模型进行高精度文本提取，并通过 Prompt 模版管理器调用大语言模型对提取内容进行结构化理解与输出，最终形成可被业务系统直接消费的标准化数据。

2. 核心需求分析

2.1. 证件识别范围及提取要素

本项目需支持多种留学相关证件的识别，涵盖身份证、护照、往来港澳通行证及多个国家的留学签证/许可类证件，具体识别证件及提取要素如下:

材料项	提取要素信息
身份证	姓名、性别、民族、身份证号码、有效期
护照个人信息页	姓名、性别、出生日期、有效期、国籍、护照号
证书	院校名，姓名，学位，专业，颁证时间
成绩单	院校名，姓名，生日，学号，学位，专业（第二主修，辅修，细分领域等），学年学期，总学分，转学分，出具日期、授课模式（full-time/part-time）

材料项	提取要素信息
（卡式）往来港澳通行证正面或（本式）往来港澳通行证首页或港澳居民来往内地通行证正面或香港、澳门永久居民身份证正面	姓名、性别、出生日期、有效期、证件号
（卡式）往来港澳通行证背面	种类、有效期、往来港澳通行证编号
（本式）逗留贴签（签注）	姓名、证件号码、有效期、前往地、“逗留”字样
电子签注	姓名、生日、“逗留、学生”字样、逗留时间、首次入境时间、院校
RPA 核查结果截图	姓名、生日、院校、文凭、专业、学位授予时间等
美国签证/许可	姓名和系统中姓名的全拼一致、签证类型中含有“F1”字样、提交存档申请时间不超过签证有效期结束时间（expiration date）
美国 I-20	姓名、签证类型是 F-1、项目结束时间（program end date）
英国签证/许可	姓名和系统中姓名的全拼一致、签证类型是“Student”、提交存档申请时间不超过 Valid until 时间
英国 CAS	姓名、有 18 位 CAS 号码、学习完成（end date）时间

材料项	提取要素信息
香港进入许可	识别到香港进入许可、包含“逗留”字样、提交存档申请时间不超过逗留签效期结束时间、姓名、证件号码、院校名称、入境时间、逗留截止时间
澳门逗留许可	识别到澳门逗留许可有效期、包含“逗留、学生”字样、提交存档申请时间不超过逗留签效期结束时间、姓名、证件号码、发出日期、逗留截止时间
澳大利亚签证	需为(granted)状态、姓名和系统中姓名拼音一致、签证类型为学生签证(500签证)、提交存档申请时间不超过 must not arrive after 时间
澳大利亚 COE	姓名、course end date 时间
加拿大签证/许可（贴签）	判断依据：上部写 CANADA；姓名和系统中姓名拼音一致、签证类型为学生签证、提交存档申请时间不超过 expiry date 时间
加拿大 Study Permit	判断依据：写 CANADA 和 STUDY PERMIT；姓名和系统中姓名拼音一致、识别到 study permit、提交存档申请时间不超过 expiry date 时间
新加坡 Student's Pass	判断依据：REPUBLIC OF SINGAPORE STUDENT'S PASS；姓名和系统中姓名拼音一致、提交存档申请时间不超过 pass expiry date 时间、识别到 student's pass
新加坡 ICA 相关许可	判断依据：上方有 ICA 及标志；姓名和系统中姓名拼音一致、提交存档申请时间不超过 Course Pre-approved till 时间
马来西亚 e-visa	判断依据：Electronic Visa eVISA Government of Malaysia；姓名和系统中姓名拼音一致、签证类型为学生签证、提交存档申请时间不超过 eVISA Expire Date 时间
马来西亚贴签	判断依据：MALAYSIA IMMIGRATION；姓名和系统中姓名拼音一致、签证类型为学生签（识别到 STUDENT）、提交存档申请时间不超过签证截止时间

2.2.用户端图像智能识别业务需求

2.2.1. 多渠道图像接入与预处理需求

1. 多渠道图像接入需求

系统具备全渠道接入、多终端图片处理能力，全面覆盖用户留学业务办理和日常办公等各类业务全流程场景。系统支持多路并发处理，可实现多终端采集图片的统一接收、解析与标准化规整处理，同时支持多用户并行上传与识别 PDF、WORD、JPG、PNG、TIFF 等多格式图片及文件的请求，确保高并发场景下实现标准化处理与格式适配，保障处理效率与服务稳定性。

2. 图像预处理与矫正引擎需求

所有接入图像均需经过统一的图像预处理引擎进行标准化处理，为后续 OCR 大模型提供高质量的输入素材。

（1）图像预处理：包含图像质量预检、版面分析区域分割等子模块，确保输入 OCR 模型的图像符合识别标准。

（2）图像质量预检：无参考感知质量评分，无需依托参考样本及深度学习模型，基于视觉感知规则完成图像质量自主量化评分，适配多类场景批量质检，评分贴合人眼判定标准；图像多维度分析，从局部细节与全局结构两大维度解析图像，精准检测画面纹理、清晰度等细节问题，研判构图、主体完整性等整体状态；支持自定义质量判定阈值，自动比对评分完成等级划分，若分值低于设定阈值系统自动触发预警。

（3）版面分析与区域分割：自动识别文档中的文字区、表格区、印章区、手写批注区；支持多栏混排、横竖混排、图文混排的版面还原；输出带坐标信息的区域切片，供 OCR 大模型进行针对性识别。

（4）证件图像的分类任务需求：针对加拿大、新加坡、马来西亚等国家各类留学相关证件，实现精准图像分类，适配留学业务办理全场景，为后续 OCR 识别、信息提取及业务审核提供精准分类支撑，确保不同国家、不同类型证件的差异化处理。

（5）其他类型材料模版的比对、匹配（通用材料分类能力）：能够识别出香港大学证书、澳门大学成绩单等。应结合文本相似度(关键词匹配、句法分析...）和图像相似度（版面结构、SSIM...）进行综合判断，以应对如申请人自拟材料的情况。当识别到不是当前业务流程所需材料，或有必要材料缺失时可即时反馈到用户端。

2.2.2. 结构化内容提取与智能语义解析需求

1. OCR 大模型文本提取引擎需求

本项目支持构建基于深度学习的 OCR 大模型识别引擎，作为结构化内容提取的底层能力底座，实现复杂版式、多语种、多类型留学材料的高精度文本提取，为上层语义解析提供高质量原文数据。

（1）识别范围与语种覆盖：支持中文（含简体、繁体）、英文常见留学相关材料的内容识别。

（2）复杂版式解析能力：具备对表格、印章、手写批注、多栏混排、横竖混排、图文混排等复杂版式的精准识别与版面还原能力；保持原文档的段落结构、表格层级、文字顺序及空间位置关系，输出带坐标信息的结构化版面数据。

（3）识别准确率指标：印刷体中文/英文识别准确率>95%，繁体中文及特殊版式识别准确率≥90%；手写体识别准确率≥80%；表格结构还原准确率≥90%。

2. Prompt 模版管理器需求

本项目支持构建可配置、可复用的 Prompt 模板库，针对不同材料类型预设结构化提取策略，实现业务规则的灵活配置与快速适配，降低技术门槛，提升业务响应效率。

（1）模板库建设与分类管理：建立面向各类留学相关材料类型的预设 Prompt 模板库；支持模板的新增、编辑、复制、删除及分类检索，形成可沉淀、可复用的业务知识资产。

（2）可视化界面配置：提供业务人员友好的可视化配置界面，支持通过表单填写、条件设置等方式调整 Prompt 规则；支持输出字段映射配置、提取规则优先级设置，无需编写代码即可完成业务适配。

（3）零代码业务适配：支持业务人员根据新材料类型或提取规则变化，在可视化界面中快速创建或调整 Prompt 模板；支持模板实时预览与效果验证，配置完成后一键发布生效，实现从需求变更到生产上线的零代码闭环。

3. 大语言模型语义锚定与关键信息抽取需求

本项目支持基于 OCR 提取的原始文本，调用大语言模型后，直接输出标准化 JSON 结构化数据，核心功能为实现从非结构化文档到结构化数据的格式转换。

（1）关键信息定位抽取：在全文识别基础上，支持基于业务规则的关键信息字段定位抽取，重点覆盖本需求书明确的各类证件提取要素。

2.2.3. 识别结果交互与质量保障需求

1. 数据实时性与严谨性保障

系统要求确保识别与结构化处理的实时性与严谨性。当用户上传的图像因质量过低（模糊、缺角、反光严重）导致 OCR 无法有效识别时，系统将即时反馈用户重新上传，而非提供潜在错误的识别结果。

2. 达到算力上限并发量时提示信息

当系统并发识别任务数接近预设上限时，系统将通过多通道实时告警机制，确保相关人员能够及时获取系统负载告警信息并采取相应措施。

3. 持续优化闭环

用户对识别结果的纠错反馈实时进入模型优化回流阶段，人工复核后用于微调 OCR 大模型与 Prompt 模板，确保输出结果的准确性。

2.2.4. 双引擎协同与知识库整合需求

1. 智能识别双引擎需求

深度整合 OCR 大模型的深度视觉理解能力及大语言模型的语义推理能力，构建"视觉+语言"双引擎架构；OCR 引擎负责像素级文本检测与识别，输出原始文本序列；LLM 引擎通过 Prompt 模版管理器对原始文本进行语义解析、字段对齐、逻辑补全，输出业务可用结构化数据；双引擎协同实现版式自适应识别、跨页信息关联级功能。

2. 多模态交互增强需求

用户可通过 PC、小程序、APP 端上传护照、港澳通行证等材料，系统基于 OCR 大模型提取全文，再通过 Prompt 模版管理器调用大语言模型综合输出结构化数据，为后续业务提供基础数据支撑。

3. 知识库与 Prompt 模板整合需求

统筹整合业务知识库及 OCR 识别规则库，搭建统一化 Prompt 模板管理体系。依托现有留学业务相关规范，整合中心业务材料标准、院校名称库、专业目录等基础资源，打造全渠道结构化 Prompt 模板平台，实现各类材料识别规则统一归集、智能适配与复用调用，有效提升图文识别精准度与业务落地适配效率。

2.3.大模型应用技术架构与算力需求

2.3.1. 大模型应用技术架构设计

大模型应用技术架构的设计统筹考量中心现有 IT 基础设施资源与业务发展现状，同时前瞻性地兼顾技术与业务的未来演进趋势。架构设计应遵循以下原则：

1. 系统整体架构要逻辑清晰、功能模块化、松耦合，具备与异构系统的集成能力和跨硬件平台的扩展能力，保障中心核心业务的持续稳定运行，并支持新业务的快速迭代部署。

2. 在安全性方面，需构建多层次纵深防护体系，确保数据全生命周期的安全可控，具备应对恶意攻击、模型逆向工程及异常交互请求等安全威胁的主动防御机制。

3. 架构设计应预留充分的技术升级空间，采用标准化接口与开放协议，以适应人工智能技术的快速发展和业务场景的持续创新需求，确保架构未来 3 年内不过时。

2.3.2. AI 算力与弹性扩展需求

提供对应本地算力服务能力，保障系统 AI 功能正常实施。

1. 算力规模需求

1）系统需支撑日均万级图像识别请求的稳定处理，单日可处理≥1 万张图片识别请求；

2）单张 A4 版式材料端到端识别（含图像预处理、OCR 文本提取、大语言模型结构化推理与格式化输出）平均响应时间≤3 秒；

3）复杂多页材料批量处理须具备并行加速能力，支持任务级并行与流水线并发，批量处理效率较串行模式提升≥60%。

4）系统需支持多路并发处理，可同时承载多路图像识别请求并行执行，确保并发场景下各项性能指标（响应时间、识别准确率）稳

定。

2. 弹性高并发服务架构

1）系统须采用分布式微服务架构设计，支持容器化部署，同时需具备弹性扩展能力的服务集群;

2）系统须整合智能负载均衡（支持加权轮询、最小连接数、一致性哈希等策略）、服务熔断降级、限流控流等容灾机制;

3）配合分布式缓存（如 Redis Cluster）与消息队列（如 Kafka/RabbitMQ）等中间件，可支撑峰值时段万级并发请求的稳定处理;

4）确保在流量峰值时段仍能提供毫秒级响应的服务体验，满足海量用户的实时交互需求，服务可用率不得低于 99.9%（排除计划内维护时段）。

3. 资源协同推进机制

1)本项目需统筹整合中心现有服务器、存储、网络等硬件设施，联动大模型专用算力（GPU/TPU/NPU 等）资源协同建设。经综合研判现有算力规模、运算性能及调度承载能力，若存量算力无法适配项目建设及业务运行需求，须开展专项算力资源补强升级，按需采购 GPU、TPU、NPU 等专业大模型算力设备，优化资源配置模式，避免资源混用造成运行低效，保障项目稳定落地运行。

2）算力资源规划须与中心现有 IT 基础设施统筹考虑，优先采用国产化技术路线（如昇腾、寒武纪等国产 AI 芯片及配套软件栈），确保自主可控。

3）算力集群须预留横向扩展接口与机柜空间，支持通过增加计算节点实现算力线性扩展，以适应后续业务增长与模型参数规模升级需求，扩容过程不得中断现有在线业务。

2.4. 系统安全性需求

1. 安全等级要求：系统须严格遵守《网络安全法》《数据安全法》《个人信息保护法》等国家网络安全相关法律法规与行业合规标准建设，满足主流网络安全防护规范与安全建设相关要求，构建完备安全防护体系，全面保障平台整体平稳可靠、安全有序运行。

2. 身份认证需求：建立统一的身份认证体系，支持OAuth2.0/OIDC标准，实现多终端、多场景的统一身份验证；采用强密码策略，支持密码复杂度校验、定期密码更换提醒；可根据需求新增双因素认证（如短信验证、令牌验证）功能，提升身份认证安全性。

3. 防越权需求：采用细粒度权限控制机制，明确不同角色的操作权限，实现权限的精准分配与管理；禁止越权访问、越权操作，对所有越权行为进行日志记录与告警；定期进行权限审计，及时清理冗余权限、违规权限，确保权限管理合规。

4. 其他安全需求：涵盖网络安全隔离、传输与存储加密（数据传输采用HTTPS协议，敏感数据存储采用加密算法）、输入输出内容审计、恶意攻击防护等；针对大模型场景，具备防范模型逆向工程、训练数据泄漏、Prompt注入攻击及敏感信息外泄的专项防护能力；建立安全日志审计机制，对所有系统操作、异常行为进行详细记录，日志留存时间符合相关要求，系统日志原则上统一留存不少于180天，包含操作日志、访问日志、识别日志、异常日志，便于安全追溯与问题排查。

2.5. 授权管理需求

为充分保障系统资产安全与使用合规性，满足私有化部署及长期稳定运行要求，系统需提供灵活、安全、可持续的授权管理机制。

1. 本地化部署授权：系统支持本地化部署模式，授权体系与部署环境绑定，确保数据不出域，满足数据主权与网络安全的合规要求。

2. 永久授权机制：系统采用一次采购、永久授权模式，授权周期无年限限制，且不设置接口调用次数上限，保障业务长期稳定运行，降低持续投入成本。

2.6.个人信息与隐私保护

1. 系统涉及证件、个人信息采集时，明确采集范围、使用目的、使用期限、存储方式。

2. 个人信息与重要数据必须境内存储，严禁出境、外传、跨境访问或处理。

3. 原始图像、识别结果、结构化数据分级权限管理，最小够用原则开放访问。

2.7.运维期需求

1. 免费运维期：项目上线后，提供1年免费运维服务，免费运维期内承担所有运维相关工作，不额外收取运维费用。

2. 运维人员要求：建设方需配备专业运维团队，运维人员需具备相关系统运维资质与经验，熟悉OCR大模型、大语言模型及相关技术架构；运维团队需提供7×24小时响应服务，针对系统出现的故障、异常，及时进行排查与处理，确保系统正常运行；定期开展系统巡检、性能优化、安全加固等工作，形成巡检报告与优化建议。

3. 运维内容：免费运维期内，负责系统日常运行维护、故障排查与修复、版本迭代更新（含材料项变化后的系统调整）、数据备份与恢复、安全漏洞修复等；提供运维培训服务，指导相关人员掌握系统运维基础操作；建立运维沟通机制，定期反馈运维情况，及时响应运维需求。

2.8.其他需求

本期 OCR 识别范围为中文简体、中文繁体、英文的材料信息，需适配各国签证材料动态变更场景，如签证办理形式调整、证件版式图案更新等情况，若出现此类业务变动，承建方须及时配合完成系统对应适配调整。

3. 实施计划

3.1.项目开发周期

本项目整体开发周期具体阶段划分如下:

1. 需求分析与原型设计阶段

针对项目需求进行系统性分析，重点聚焦于基于 OCR 大模型应用的功能定位、性能指标及用户体验标准的精准界定；通过需求调研与需求分析，完成需求文档编写、Prompt 模板体系设计及与业务系统的接口规范定义。

2. 训练数据准备与模型微调阶段

开展样本数据处理、模型专项优化及业务规则库建设；完成对各类证件、成绩单、学位证等材料样本数据的接收、清洗、脱敏校验及质量分级，形成符合模型训练要求的标准化数据集；基于业务样本开展 OCR 大模型微调，针对各地区材料版式特征进行专项优化；建立统一的图像质量分级标准与数据标注规范，形成模型效果评估基准体系。

3. 系统开发与集成测试阶段

基于前期成果，开展系统全方位功能开发与优化，重点打造多渠道图像接入与预处理系统、OCR 大模型识别引擎、Prompt 模版管理器与结构化输出引擎、管理端识别任务监控与数据埋点系统四大核心模块；开发完成后，进行全面的功能测试、性能测试、识别准确率测试

及用户体验测试，确保系统运行稳定、响应迅速、操作流畅；完成系统间联调测试，验证数据流转完整性。

4. 上线推广与持续运营阶段

完成系统上线部署，开展上线推广工作；建立完善的用户反馈机制，持续收集用户使用数据及建议，迭代优化 OCR 大模型与 Prompt 模板效果；进入免费运维期，开展日常运维工作，保障系统稳定运行。

3.2. 开发人员需求

建设方需配备专业的开发团队，团队人员配置及要求如下：

1. 项目负责人 1 名：具备 5 年以上 AI 项目管理经验，熟悉 OCR 大模型、大语言模型相关项目开发流程，能够统筹项目进度、协调资源，确保项目按时按质完成。

2. 算法工程师 1 名：具备 3 年以上 OCR、NLP 相关算法开发经验，熟悉深度学习框架，能够完成 OCR 大模型微调、Prompt 工程优化、关键信息抽取算法开发等工作。

3. 前端开发工程师 1 名：具备 3 年以上前端开发经验，熟悉现代化前端框架（如 Vue、React），能够完成多终端交互开发、优化。

4. 后端开发工程师 2 名：具备 3 年以上分布式微服务开发经验，熟悉 Java/Python 等开发语言，能够完成系统架构搭建、接口开发、服务集群部署等工作。

5. 测试工程师 1 名：具备 3 年以上软件测试经验，熟悉功能测试、性能测试、安全测试流程，能够完成系统全面测试，排查潜在问题，确保系统质量。

6. 运维工程师 1 名：具备 3 年以上系统运维经验，熟悉服务器、容器化部署、网络安全等相关知识，能够完成系统部署、日常运维、故障排查等工作，满足运维期服务要求。

4. 风险评估与应对策略

需具备对风险场景具备评估和制定应对策略的能力，以下为在项目开发中和上线后可能会遇到的风险。

4.1. OCR 识别准确率风险

（一）风险评估

识别准确率波动：港澳地区特殊版式、手写体、低质量扫描件等场景可能导致识别准确率下降，影响后续结构化输出质量。

（二）应对策略

1）数据增强与模型微调

针对港澳材料样本建立专项样本库，持续补充训练数据；采用数据增强技术（旋转、模糊、光照变换）提升模型鲁棒性；对低置信度结果自动触发人工复核流程，确保输出质量。

4.2. 数据安全与隐私风险

（一）风险评估

用户上传的护照、成绩单等敏感信息可能面临泄漏风险。跨境数据流动（如港澳地区数据）需符合相关法规要求。

（二）应对策略

1）加密存储与传输

使用端到端加密技术，严格限制数据访问权限，原始图像与识别结果分级存储。

2）合规性设计

明确数据使用边界，提供用户数据删除选项，确保符合目标地区隐私法规及中心数据安全规范。

4.3. 技术融合风险

（一）风险评估

技术实现复杂度高: OCR 大模型与大语言模型的协同、Prompt 工程的稳定性、多源异构数据的结构化映射涉及多技术融合（CV、NLP、Prompt Engineering），开发难度大。

数据依赖性强:系统需整合多源数据（材料版式库、业务字段库、院校数据库等），数据质量或接口稳定性可能影响功能实现。

（二）应对策略

1）分阶段开发

优先实现核心识别与结构化功能，逐步迭代高级版式（如手写体、复杂表格）适配。

4.4.运营与维护风险

（一）风险评估

识别规则库与 Prompt 模板更新滞后（如港澳新版式材料出现）导致识别信息不准确，影响用户体验。

（二）应对策略

1）建立动态更新机制

实时获取材料版式变化数据，设置自动提醒人工审核与 Prompt 模板迭代。

4.5.业务衔接风险

（一）风险评估

本项目负责数据提取及图像预处理矫正；业务系统承担后续处理。若接口规范不清晰或数据格式不统一，可能导致系统间衔接不畅。

（二）应对策略

1）标准化接口设计

在项目初期与业务系统团队联合制定《数据交换接口规范》，明确字段定义、格式标准、传输协议。

2）联调测试机制

在系统测试阶段安排专项联调测试，验证端到端数据流转完整性。

3）责任边界固化

通过技术文档与服务级别协议（SLA）明确双方责任边界，确保"预处理提取"与"业务消费"环节无缝衔接。

5. 结论

本项目拟建设的 OCR 大模型智能识别系统，将深度整合先进 OCR 大模型技术与大语言模型的语义理解、结构化输出能力，实现身份证、护照、往来港澳通行证及各国留学签证/许可等材料图像的智能化识别与数据挖掘。

产品核心功能包括：对接 PC 端、小程序端、APP 端的多渠道图像接入（支持多路并发）；图像预处理、版面分析；基于 OCR 大模型实现中文（含简体、繁体）、英文材料的高精度文本提取；通过 Prompt 模版管理器调用大语言模型对提取内容进行结构化输出；与现有业务系统实现标准化数据对接。同时，项目将满足系统安全等级、身份认证、防越权等安全需求，提供 1 年免费运维服务，配备专业开发与运维团队，确保项目按时落地、稳定运行，为留学相关业务提供高质量的数据支撑。

附件 2

OCR 大模型智能识别系统
数据安全和保密协议

本《数据安全和保密协议》(“**本协议**”)由以下双方于【2026】年【9】月【30】日于北京市【海淀】区签署:

甲方：教育部留学服务中心

住　所　地：北京市海淀区北四环西路 56 号辉煌时代大厦 10 层

法定代表人：李　智

项目联系人：吴明栋

通讯地址：北京市海淀区北四环西路 56 号辉煌时代大厦 10 层

邮政编码：100080

电话：010-62677915

乙方：讯飞智元信息科技有限公司

住所地：安徽省合肥市高新区云飞路 66 号天源迪科 1 号楼 5-8 层

法定代表人：张友国

项目联系人：袁磊

通讯地址：

邮政编码：230001

电话：0551-65309171

传真：0551-65309171

本协议中，甲方、乙方单称“一方”，合称“双方”。

本着平等互利的原则，经双方友好平等协商一致，就【OCR 大模型智能识别系统项目】（“本项目”）自愿签订本协议，以资双方共同信守。

一、保密内容和范围

乙方应承担保密义务的范围包括但不限于:

1. 软件系统建设过程中，可接触到的任何关于甲方的数据和信息，包括直接、间接、口头或书面等形式;

2. 依照法律规定或有关协议的约定，其他需承担保密义务的事项。

乙方应承担保密义务的范围不适用于如下信息:

1）非由于乙方的原因已经为公众所知的;

2）由于法律的适用、法院或其他国家权力机关的要求而披露的信息。

3.任何一方应对提供本合作过程中知悉的对方的商业秘密（包括但不限于商业信息、数据、程序、合同、经营决策等信息）、对方提供的文件资料及对方要求保密的其他信息（以下简称“保密信息”）承担保密义务，并采取相应的保密措施。任何一方应承担的保密义务包括但不限于:

1）未经对方书面同意，不得将上述商业秘密、文件资料和其他信息披露给任何第三人;

2）不得将上述商业秘密，文件资料和信息用于本合同

以外的其他目的;

3）在本合同终止后或按对方要求，及时将上述文件资料和信息返还对方，不得备份留存。

4）乙方承诺对系统开发过程中所获得的技术、甲方在本合同期内任何时候或为了系统开发的洽谈而对其提供或披露的任何专有的资料和信息以及在系统中存储的各类数据保守秘密，专有接口不对第三方等均不得向任何第三方或人士披露和使用。

4. 双方了解并承诺，一方提供、披露之保密信息或因进行共同合作所知悉、持有之保密信息，均仅供实现本合同的目的使用。任何一方不得将保密信息披露、公布、散布或分发给除了实现本合同目的必须使用该保密信息的员工或专业顾问之外的任何第三方，提供程度仅限于可执行本协议目的。双方应事先与员工及专业顾问签署不低于本合同保密义务的长期有效的保密协议，保证该员工或专业顾问遵守本合同约定的义务。若前述人员有违反本协议规定的情况，即视为该方的违约行为。

5. 双方保证已根据有关数据保护法律的要求，建立了适当的数据安全能力，落实了必要的管理和技术措施，以防止数据的泄露、损毁、丢失、篡改。双方应当互相配合，确保数据合作过程中不会造成任何的数据泄露、损毁、丢失或篡改。如果数据进入任何一方指定的系统或任何存储空间后，

发生任何数据泄露、损毁、丢失或篡改等数据安全事件，其相关的全部责任由该方承担。

6. 在任何情况下，任何一方须以保护己方具有同等敏感性和重要性的保密信息时所使用的谨慎程度（至少不低于合理的谨慎程度）来保护对方的保密信息。一经发现其保管的保密信息受到任何未经授权的披露或有被泄露的危险时，应尽快通知对方，并同时尽最大努力防止对该等保密信息的任何进一步披露或未经授权的使用。

7. 如果根据法律程序或行政强制性要求必须披露保密信息，则应在接到强制披露要求后，在披露前，均应事先书面通知对方，以便对方寻求必要的保护措施，防止或限制保密信息的进一步扩散；若一方被强制要求直接向执法部门披露，应在法律程序或行政要求所允许的最小范围内披露该“保密信息”，并向对方提供相关保密信息的副本。

8. IP 地址和域名：

1）乙方采取一切合理可行的措施，确保其分配给甲方使用的 IP 地址和域名归属清晰、合法，并符合国家关于互联网 IP 地址和域名管理的相关法规要求；

2）乙方定期对所提供的 IP 地址和域名进行安全审查，至少每个季度进行一次全面的安全评估，如若发现安全隐患及时通知甲方；

3）若因乙方未能妥善管理 IP 地址和域名导致甲方遭受

外部攻击或数据泄露和数据安全保密问题，乙方应在遇到此类问题立刻向甲方报备，并响应解决或接到甲方通知后 4 小时内响应解决，并协助甲方采取紧急措施限制损害的进一步扩大，如遇 IP 地址和域名归属问题风险，公网暴露风险或由于乙方未能妥善管理 IP 地址和域名导致甲方遭受外部攻击导致的数据泄露和数据安全保密问题，乙方需承担全部责任;

4）乙方负责维护甲方使用 IP 的网络环境安全，防止未授权访问，并保证网络服务的连续性和稳定性。

9. 业务数据安全和保密:

1）乙方提供安全加密的网络传输协议接口，保障数据安全传输;

2）乙方确保其技术服务团队所有成员应当履行本协议约定的保密义务。凡是在工作过程中所接触或知悉的关于甲方的所有信息均应负有保密义务，不得以任何形式传播，且保密协议不受服务期限的限制。乙方在未授权的情况下不得利用甲方内部数据进行模型训练。因乙方的原因发生网络安全和数据泄露等安全事件等，乙方须承担相应法律责任，并赔偿甲方相应损失;

3）甲方有权定期或不定期对乙方的数据保密措施进行审查，以确保乙方严格遵守保密协议。如发现违反保密义务的情形，甲方有权要求乙方立即纠正，并对因此造成的损失

有权要求赔偿。

10. 定期安全巡检和技术加固:

需对系统的应用层、网络层以及数据库层等进行技术加固，日常提升管理和加强主动防御能力，并建立长效安全协作机制，定期检查并向我中心汇报安全态势。

二、双方权利与义务、责任

就本协议所约定的保密内容，乙方承担以下保密义务:

1. 不得刺探、截取与本项目无关的数据信息;

2. 不得利用所掌握的数据信息谋取私利;

3. 不得向与本项目无关的任何第三人披露甲方的数据信息;

4. 不得允许或协助与本项目无关的任何第三人使用甲方的数据;

5. 如发现数据被泄露，应当立即采取有效措施防止进一步扩大，尽最大可能消除影响并及时向甲方报告；未及时采取有效措施所造成的损失，应当由受托人承担;

6. 未经甲方事先书面许可，不得擅自进入项目专用服务器或修改相关信息;

7. 乙方技术人员需要连接项目专用服务器进行调试或软件的日常维护工作前，需提前经甲方同意，并告知甲方本次工作内容及目的。

三、违约与赔偿

1. 除了不可抗力外（指地震、台风、火灾、水灾、战争、罢工、黑客攻击以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况），若任何一方违反本协议约定的保密义务，应在第一时间采取一切必要措施防止保密信息的扩散，尽最大可能消除影响，并应承担违约责任，违约方一次性向守约方支付该项目金额的 30%的违约金。

2. 上述违约金数额并不影响守约方向违约方要求损害赔偿，包括但不限于守约方因调查违约行为而产生的合理费用。

3. 因乙方技术团队成员违反本协议保密义务，由乙方承担全部法律责任。给甲方造成实际经济损失的，由乙方承担赔偿责任。

四、保密期限

本协议自签订之日起生效，并持续有效，双方协商一致可终止协议。双方合作项目的终止并不影响协议的效力，本保密条款以及其项下义务应在双方合作期限届满或终止后持续有效，自保密信息权利人自行将保密信息公开之日止。

五、争议解决

因执行本协议或与本协议相关的任何纠纷，可通过双方友好协商解决或共同委托双方信任的第三方调解。协商、调解不成或者一方不愿意协商、调解的，任何一方可向甲方所在地人民法院提起诉讼。

六、其他

本协议一式四份，双方各执两份，自甲乙双方加盖公章或合同专用章且法定代表人或授权代表签字之日起立即生效。传真件与原件同样具有法律效力。