**Product Requirement Document: AutoResLMA (Automated Research with LLM Agents)**

**Version:** 1.0 **Date:** May 19, 2025 **Author:** [Your Name/Team Name] **Status:** Draft

**(Suggestion: As we develop this, we can refine versioning and add more specific authors/stakeholders.)**

**1. Introduction & Overview**

* **1.1. Project Purpose:** AutoResLMA aims to evolve the existing "slr-automation" tool into a comprehensive, AI-powered platform that assists researchers throughout the entire scientific research lifecycle.
* **1.2. Vision:** Inspired by the "A Vision for Auto Research with LLM Agents" paper, AutoResLMA envisions a structured multi-agent framework designed to leverage specialized Large Language Model (LLM) agents to automate, coordinate, and optimize various phases of the research process, from preliminary literature review to dissemination of findings. This platform will act as an intelligent assistant to human researchers, enhancing productivity and potentially accelerating discovery.
* **1.3. Current State:** The foundational "slr-automation" tool provides capabilities for systematic literature review (SLR) automation, including research question generation, search string creation, paper fetching/filtering, answer generation, and summary creation. This PRD outlines the expansion of these capabilities into a broader, agent-based system.
* **1.4. Scope:** This document outlines the requirements for the phased development of AutoResLMA, detailing the features, functionalities, and technical considerations for transforming the current application.

**(Suggestion: Consider adding a glossary of terms if specific terminology from the "AutoResearch Vision" paper or internal project terms will be used extensively.)**

**2. Goals & Objectives**

* **2.1. Primary Goals:**
  + To significantly reduce the manual effort and time involved in various stages of the research lifecycle.
  + To provide researchers with intelligent tools that augment their capabilities in literature analysis, idea generation, methodological planning, paper development, and dissemination.
  + To create an integrated and cohesive research pipeline where information flows seamlessly between different research stages and AI agents.
* **2.2. Secondary Objectives:**
  + To improve the consistency and thoroughness of literature reviews.
  + To assist in identifying novel research gaps and formulating robust research questions/hypotheses.
  + To streamline the process of drafting and refining research manuscripts.
  + To explore the potential of LLM agents in various research tasks while emphasizing human oversight and control.
  + To foster a collaborative environment where AI agents support human researchers.

**3. Target Audience**

* **3.1. Primary Users:**
  + Academic Researchers (across various disciplines).
  + PhD students and Post-doctoral researchers.
  + Early-career researchers.
* **3.2. Secondary Users:**
  + Research teams and consortia.
  + Industry researchers involved in R&D.
  + Independent scholars.

**4. Key Features (Aligned with "AutoResearch Vision" Agents & Phases)**

This section outlines features to be developed in a phased approach.

* **Phase 0: Foundational Enhancements & Agent Refactoring**
  + **F0.1: Enhanced SLR Core:**
    - F0.1.1: Improved LLM prompt engineering for existing SLR features (RQs, search strings, summaries) for higher accuracy and control.
    - F0.1.2: Advanced user-defined inclusion/exclusion criteria for AI paper filtering.
    - F0.1.3: Module for LLM-assisted quality assessment of selected papers in an SLR (e.g., based on user-provided checklists).
  + **F0.2: System Architecture:**
    - F0.2.1: Refactor existing backend Python scripts (agents.py, agents2.py, etc.) into a modular, class-based structure representing individual "Specialized Research Agents."
    - F0.2.2: Implement robust state management for data persistence and flow across different research stages/agents.
    - F0.2.3: Develop a basic internal workflow engine or data passing mechanism between agents.
  + **F0.3: UI/UX Enhancements:**
    - F0.3.1: Improved navigation and user experience for the existing SLR workflow.
    - F0.3.2: Design initial UI concepts for a multi-agent, multi-stage research dashboard.
* **Phase 1: "Preliminary Research" Agents (Steps 1, 2, 3 of AutoResearch Vision)**
  + **F1.1: Literature Agent (Enhanced)** (Corresponds to Step 1)
    - F1.1.1: Automatically identify and list potential research gaps based on the synthesized literature from the SLR.
    - F1.1.2: Provide more structured and interconnected knowledge synthesis from the literature (beyond simple summaries).
  + **F1.2: Idea Agent** (Corresponds to Step 2)
    - F1.2.1: Accept identified research gaps (from Literature Agent) or user-defined broad topics as input.
    - F1.2.2: Generate novel research questions and/or testable hypotheses using various idea generation patterns (e.g., problem decomposition, applying new techniques to existing problems, as inspired by Figure 3 in "AutoResearch Vision").
    - F1.2.3: Allow users to review, refine, rate, and select generated ideas/hypotheses.
  + **F1.3: Method Agent (Initial - Method Planning)** (Corresponds to Step 3)
    - F1.3.1: Based on a selected idea/hypothesis (from Idea Agent), generate a high-level research plan (sequence of steps) as per Figure 2 in "AutoResearch Vision."
    - F1.3.2: For each step in the high-level plan, suggest appropriate research methodologies (e.g., SLR protocol elements, survey design, experimental setup outline).
    - F1.3.3: Provide justifications, pros, and cons for suggested methodologies.
    - F1.3.4: Allow users to select and customize the methodological approach.
* **Phase 2: "Empirical Study" Agent (Initial - Step 4)**
  + **F2.1: Experiment Agent (Initial - High-Level Design & Planning)** (Corresponds to Step 4)
    - F2.1.1: Assist in designing the chosen empirical method:
      * Identify and define key variables (independent, dependent, control).
      * Outline participant groups or sample characteristics.
      * Draft a procedural outline for the study.
    - F2.1.2 (Experimental/Future): Suggest algorithms or generate boilerplate code for computational studies or simulations, if applicable.
    - F2.1.3: Assist in drafting a data collection plan (how data will be gathered).
    - F2.1.4: Suggest appropriate data analysis techniques (statistical tests, qualitative approaches) based on the method and expected data types.
    - F2.1.5: Prompt for and help outline ethical considerations for the planned study. *(Human oversight is critical for all F2.1 features)*
* **Phase 3: Enhanced "Paper Development" Agents (Steps 5, 6, 7)**
  + **F3.1: Paper Agent (Enhanced)** (Corresponds to Step 5)
    - F3.1.1: Integrate summaries of planned empirical work (from Experiment Agent) into the relevant paper sections (e.g., Methods, proposed Results).
    - F3.1.2: Suggest appropriate structure for different paper sections based on research type (SLR, empirical study).
    - F3.1.3: Suggest potential visualizations (types of charts, tables) based on planned data and analysis.
    - F3.1.4: Enhance LaTeX output to be more dynamic and accommodate richer content.
  + **F3.2: Evaluation Agent** (Corresponds to Step 6)
    - F3.2.1: Perform automated self-critique of the drafted manuscript (by Paper Agent) for coherence, logical flow, clarity, and alignment with initial research questions and methods.
    - F3.2.2 (Optional Integration): Integrate with third-party plagiarism detection services.
    - F3.2.3 (Optional Integration): Integrate with third-party advanced grammar and style checking services.
    - F3.2.4: Allow users to input journal/conference review criteria, against which the agent attempts to assess the draft.
  + **F3.3: Rebuttal Agent** (Corresponds to Step 7)
    - F3.3.1: Allow users to upload or input reviewer comments.
    - F3.3.2: Assist in categorizing and summarizing reviewer comments.
    - F3.3.3: Suggest potential responses to comments, referencing relevant sections of the drafted paper or outputs from other agents (Literature, Method, etc.).
    - F3.3.4: Help draft polite and constructive responses to reviewer feedback.
* **Phase 4: "Dissemination" Agent (Step 8)**
  + **F4.1: Promotion Agent** (Corresponds to Step 8)
    - F4.1.1: Generate plain language summaries of the research findings suitable for broader audiences.
    - F4.1.2: Create outlines or draft content for presentations (e.g., key talking points per slide).
    - F4.1.3: Draft posts for social media or academic networking platforms to share findings.
    - F4.1.4: Suggest relevant keywords for indexing and discoverability of the research paper.
    - F4.1.5 (Experimental/Future): Based on the paper's content and bibliography, suggest potential target journals or conferences.

**(Suggestion: For each feature, consider adding a "Priority" (e.g., Must-have, Should-have, Could-have, Won't-have for this version/phase) to help with roadmap planning.)**

**5. User Stories**

* **Phase 0 & 1 (Researcher focusing on SLR and Idea Generation):**
  + "As a PhD student, I want to input my research objective and have the **Literature Agent** provide me with relevant papers, a synthesis of current knowledge, and a list of identified research gaps, so that I can quickly understand the state-of-the-art."
  + "As an early-career researcher, I want the **Idea Agent** to suggest novel research questions based on the gaps identified by the Literature Agent, so I can explore promising new research directions."
  + "As a researcher, I want the **Method Agent** to help me draft a detailed SLR protocol, including inclusion/exclusion criteria and quality assessment steps, based on my selected research questions, so I can ensure my review is systematic and rigorous."
* **Phase 2 (Researcher planning an empirical study):**
  + "As a researcher, after the **Idea Agent** helped me formulate a hypothesis, I want the **Method Agent** to suggest suitable empirical methodologies and then help me outline the experimental design using the **Experiment Agent**, so I can plan my study effectively."
  + "As a researcher, I want the **Experiment Agent** to help me draft a data analysis plan relevant to my proposed experimental design, so I can think ahead about how I will interpret my results."
* **Phase 3 (Researcher writing and refining a paper):**
  + "As an academic, I want the **Paper Agent** to help me draft the introduction and methods sections of my paper by integrating information from the Literature, Idea, and Method agents, so I can save time on initial drafting."
  + "As a researcher, I want the **Evaluation Agent** to review my drafted paper for coherence and clarity before I send it to colleagues, so I can improve its quality."
  + "As a researcher, after receiving peer review feedback, I want the **Rebuttal Agent** to help me organize the comments and draft initial responses, so I can address the feedback more efficiently."
* **Phase 4 (Researcher disseminating work):**
  + "As a researcher, once my paper is accepted, I want the **Promotion Agent** to generate a plain language summary and a few social media posts, so I can easily share my findings with a wider audience."

**(Suggestion: Develop more detailed user stories for each specific feature as development for that feature approaches. Consider different user personas within the "researcher" category.)**

**6. Technical Requirements**

* **6.1. Architecture:**
  + Modular, agent-based backend architecture (Python, Flask).
  + Microservices or clearly separated modules for each Specialized Research Agent.
  + RESTful APIs for communication between frontend and backend agents.
  + Scalable infrastructure to handle potentially long-running LLM tasks and concurrent users.
* **6.2. Backend:**
  + Python (Flask or similar framework).
  + Integration with multiple LLM APIs (OpenAI, DeepSeek, and potentially others). Must handle different API schemas and capabilities.
  + Database for persistent storage of user projects, research artifacts (literature, ideas, methods, drafts), agent states, and user accounts (e.g., PostgreSQL, MongoDB).
  + Vector database (e.g., Pinecone, Weaviate) for semantic search over project documents and literature to support agent reasoning.
  + Task queuing system (e.g., Celery, Redis Queue) for managing asynchronous LLM calls and long-running processes.
* **6.3. Frontend:**
  + Modern JavaScript framework (e.g., React – current stack, Vue, or Angular).
  + User-friendly interface for managing multi-stage research projects.
  + Interactive elements for reviewing, editing, and approving AI-generated content.
  + Real-time updates for long-running tasks.
* **6.4. LLM Integration:**
  + Flexible system to accommodate different LLMs and switch between them.
  + Advanced prompt engineering and context management strategies.
  + Mechanisms for handling LLM rate limits, errors, and varying response structures.
* **6.5. Security:**
  + Secure handling of API keys for LLMs and other services.
  + User authentication and authorization.
  + Protection against common web vulnerabilities.
  + Consideration for data privacy, especially if users upload sensitive research data.
* **6.6. Deployment:**
  + Containerization (e.g., Docker, Kubernetes) for easier deployment and scaling.
  + CI/CD pipeline for automated testing and deployment.

**7. Success Metrics**

* **7.1. Adoption & Usage:**
  + Number of registered users.
  + Number of active research projects created.
  + Frequency and duration of user sessions.
  + Completion rates for each stage of the research lifecycle within the platform.
* **7.2. User Satisfaction:**
  + User feedback surveys (e.g., Net Promoter Score - NPS, satisfaction with specific agents/features).
  + Qualitative feedback from user interviews.
  + Reduction in reported time spent on specific research tasks compared to manual methods.
* **7.3. Quality of Output:**
  + User ratings of the quality and relevance of AI-generated content (RQs, summaries, drafts).
  + (Long-term) Case studies or testimonials of successful research outputs facilitated by the platform.
* **7.4. System Performance:**
  + Average response time for AI agent tasks.
  + System uptime and reliability.
  + Scalability under increasing load.

**(Suggestion: Define specific, measurable, achievable, relevant, and time-bound (SMART) goals for some of these metrics, especially for initial phases.)**

**8. Potential Risks & Dependencies**

* **8.1. Risks:**
  + **LLM Reliability & Accuracy:** LLMs can hallucinate or produce biased/incorrect information. Heavy reliance on human oversight is needed.
  + **Scientific Rigor:** Ensuring agent-generated research (especially methods, experiments, evaluations) meets high scientific standards is a major challenge.
  + **Over-Automation & Deskilling:** Users might become overly reliant on the tool, potentially diminishing critical thinking skills.
  + **Ethical Concerns:** Authorship (AI vs. human), intellectual property of AI-generated content, potential for misuse in generating low-quality or fabricated research.
  + **Technical Complexity:** Building a robust, multi-agent system with complex LLM integrations is technically challenging.
  + **Cost of LLM APIs:** Extensive use of powerful LLMs can be expensive.
  + **User Adoption:** Researchers may be hesitant to adopt new, AI-driven tools that change established workflows.
  + **Integration Challenges:** Integrating various LLMs and third-party services smoothly.
  + **Scalability Issues:** Handling a large number of users and complex, long-running tasks.
* **8.2. Dependencies:**
  + Availability and stability of third-party LLM APIs (OpenAI, DeepSeek, etc.).
  + Availability of academic search APIs (Scopus, Semantic Scholar) and their terms of service.
  + Continued advancements in LLM capabilities for more complex reasoning and generation tasks.
  + Skilled development team with expertise in AI/ML, backend/frontend development, and potentially research methodologies.
  + Clear user feedback and involvement throughout the development process.

**9. Future Considerations / Out of Scope (for initial MVP / Phased Rollout)**

* **Phase 0 will be the initial focus, building upon "slr-automation."**
* **Initial releases of Phases 1-4 may not include all sub-features listed.** Prioritization will be key.
* **Direct execution of empirical experiments or primary data collection by AI agents** is explicitly out of scope for the foreseeable future; the focus is on planning and assistance.
* **Advanced, fully autonomous agent collaboration with minimal human intervention** is a long-term vision, not an initial requirement.
* **Deep domain-specific knowledge bases pre-built into agents** (beyond what LLMs inherently possess) might be a future enhancement.
* **Full automation of peer review or grant proposal writing** is out of scope for initial phases.

**(Suggestion: This PRD is quite comprehensive. For actual development, it would be broken down into smaller PRDs or feature specifications for each phase or even each major agent. This document serves as the overarching vision and requirement set.)**

This PRD provides a detailed blueprint for developing AutoResLMA. Remember that this is a living document and should be updated as the project progresses, requirements evolve, and more is learned from user feedback and technological advancements.