SaaS Application Requirements

1. **User Authentication and Login**

* **Functional Requirements:**
  + Secure user registration and login (email/password, OAuth, or SSO).
  + Password reset and account recovery mechanisms.
* **Security Requirements:**
  + Enforce strong password policies.
  + Implement multi-factor authentication (MFA).
  + Encrypt passwords at rest using industry-standard hashing (e.g., bcrypt).
  + Protect against brute force and credential stuffing attacks.
  + Use HTTPS for all data transmission.

2. **Intake Form**

* **Functional Requirements:**
  + Form fields: Job Description (text), Job Title (text), Base Resume (file upload or text).
  + Input validation for all fields.
* **Security Requirements:**
  + Sanitize and validate all user input to prevent injection attacks.
  + Scan uploaded files for malware and restrict file types.
  + Store uploaded resumes securely (encrypted at rest).
  + Limit file upload size and rate to prevent DoS attacks.

3. **Job Aggregation from LinkedIn**

* **Functional Requirements:**
  + Connect to LinkedIn API to fetch relevant job postings based on intake form data.
  + Display aggregated job listings to the user.
* **Security Requirements:**
  + Use secure API authentication (OAuth 2.0).
  + Never store user LinkedIn credentials; use tokens.
  + Limit API request rates to avoid abuse and comply with LinkedIn’s terms.
  + Log and monitor API interactions for anomalies.

4. **Resume and Cover Letter Customization**

* **Functional Requirements:**
  + For each job, generate a tailored resume and cover letter using AI.
  + Allow user to review and edit generated documents.
  + Provide templates and formatting options.
* **Security Requirements:**
  + Ensure AI processing is isolated per user (no data leakage).
  + Encrypt all generated documents at rest.
  + Prevent unauthorized access to user documents.
  + Log all document generation and access events.

5. **Interview Preparation**

* **Functional Requirements:**
  + Analyze job description to generate interview questions and tips.
  + Provide company-specific insights and likely interview topics.
* **Security Requirements:**
  + Protect user data privacy during analysis.
  + Ensure all external data sources (e.g., company info APIs) are accessed securely.
  + Do not store unnecessary personal or proprietary data.

6. **Company Insights from Reddit**

* **Functional Requirements:**
  + Search Reddit for company reviews, interview experiences, and past questions.
  + Summarize and present relevant findings to the user.
* **Security Requirements:**
  + Use Reddit’s official API with secure authentication.
  + Filter and moderate content to avoid displaying inappropriate or malicious information.
  + Respect Reddit’s API usage limits and privacy guidelines.

7. **General Application Security**

* **Requirements:**
  + Role-based access control (RBAC) for users and admins.
  + Comprehensive logging and monitoring of all user and system activities.
  + Regular security audits and vulnerability assessments.
  + Compliance with relevant data privacy laws (e.g., GDPR, CCPA).
  + Incident response plan for data breaches or security incidents.
  + Secure deployment practices (e.g., containerization, automated patching).

Summary Table

| **Functional Area** | **Functional Requirements (Summary)** | **Security Requirements (Summary)** |
| --- | --- | --- |
| Authentication/Login | User registration, login, password reset | Strong passwords, MFA, encryption, HTTPS, brute force protection |
| Intake Form | Job description, title, base resume input | Input validation, file scanning, encryption, DoS protection |
| LinkedIn Aggregation | Fetch jobs from LinkedIn API | Secure API use, no credential storage, rate limiting |
| Resume/Cover Letter AI | Customization per job, templates, editing | Data isolation, encryption, access controls, logging |
| Interview Prep | Generate questions/tips, company insights | Data privacy, secure API use, minimal data storage |
| Reddit Insights | Fetch/summarize company info and interview experiences | Secure API, content moderation, privacy compliance |
| General Security | N/A | RBAC, logging, audits, compliance, incident response |

This structure ensures each feature is paired with clear, actionable security requirements, aligning with best practices for SaaS and sensitive user data protection.