5. Non-Functional Requirements

This section specifies the non-functional requirements for the AI-Driven Job Matching Platform. These requirements define the quality attributes and constraints that the system must satisfy to meet stakeholder expectations.

5.1. Performance Requirements

5.1.1. Response Time

ID	Requirement
NFR-01.	The system SHALL provide page load times of less than 3 seconds for standard operations under normal load conditions.
NFR-02.	The system SHALL provide search results within 2 seconds for standard search queries.
NFR-03.	The system SHALL complete AI matching operations within 5 seconds for individual job-candidate matches.
NFR-04.	The system SHALL process batch operations (e.g., bulk candidate matching) within a timeframe proportional to the batch size, not exceeding 2 minutes for standard operations.
NFR-05.	The system SHALL maintain response time degradation of no more than 50% during peak load periods.

5.1.2. Throughput

ID	Requirement
NFR-06.	The system SHALL support at least 1,000 concurrent users during normal operations.
NFR-07.	The system SHALL support at least 5,000 concurrent users during peak periods.
NFR-08.	The system SHALL process at least 100 job applications per minute during peak periods.
NFR-09.	The system SHALL support at least 500 new job postings per day.
NFR-10.	The system SHALL support at least 1,000 new user registrations per day.

5.1.3. Resource Utilization

ID	Requirement
NFR-11.	The system SHALL operate within the allocated server resources, utilizing no more than 80% of CPU capacity during normal operations.
NFR-12.	The system SHALL utilize no more than 80% of available memory during normal operations.
NFR-13.	The system SHALL require no more than 5TB of storage for the first year of operation, with a growth plan for subsequent years.
NFR-14.	The system SHALL optimize database queries to minimize I/O operations and response times.
NFR-15.	The system SHALL implement caching mechanisms to reduce resource utilization for frequently accessed data.

5.1.4. Scalability

ID	Requirement
NFR-16.	The system **SHALL** be designed to scale horizontally by adding more server instances to handle increased load.
NFR-17.	The system **SHALL** be designed to scale vertically by utilizing additional resources on existing servers.
NFR-18.	The system **SHALL** support a minimum of 100,000 registered job seekers without performance degradation.
NFR-19.	The system **SHALL** support a minimum of 10,000 registered employers without performance degradation.
NFR-20.	The system **SHALL** support a minimum of 50,000 active job postings without performance degradation.
NFR-21.	The system **SHALL** be designed to accommodate a 100% annual growth in user base and transaction volume for at least the first three years of operation.

5.2. Security Requirements

5.2.1. Authentication and Authorization

ID	Requirement
NFR-22.	The system **SHALL** implement multi-factor authentication for administrative accounts and as an option for all users.
NFR-23.	The system **SHALL** enforce strong password policies, including minimum length, complexity, and regular password changes.
NFR-24.	The system **SHALL** implement role-based access control (RBAC) to restrict access to features and data based on user roles.
NFR-25.	The system **SHALL** maintain detailed access logs for all authentication and authorization events.
NFR-26.	The system **SHALL** automatically lock accounts after a specified number of failed login attempts.
NFR-27.	The system **SHALL** implement secure session management with appropriate timeout settings.
NFR-28.	The system **SHALL** support OAuth 2.0 and OpenID Connect for third-party authentication where applicable.

5.2.2. Data Protection

ID	Requirement
NFR-29.	The system **SHALL** encrypt all sensitive data at rest using industry-standard encryption algorithms (AES-256 or equivalent).
NFR-30.	The system **SHALL** encrypt all data in transit using TLS 1.3 or higher.
NFR-31.	The system **SHALL** implement data masking for sensitive information displayed in the user interface.
NFR-32.	The system **SHALL** implement secure key management practices for encryption keys.
NFR-33.	The system **SHALL** provide mechanisms for secure data deletion when required.
NFR-34.	The system **SHALL** implement database-level encryption for sensitive tables and columns.

NFR-35.	The system **SHALL** maintain separate environments for development, testing, and production with appropriate data isolation.

5.2.3. Privacy and Compliance

ID	**Requirement**
NFR-36.	The system **SHALL** comply with Palestinian data protection regulations and incorporate GDPR principles as best practice.
NFR-37.	The system **SHALL** provide mechanisms for users to view, export, and delete their personal data in accordance with data protection regulations.
NFR-38.	The system **SHALL** maintain audit trails of all data access and modifications for compliance purposes.
NFR-39.	The system **SHALL** implement data minimization principles, collecting only necessary information for system functionality.
NFR-40.	The system **SHALL** provide clear privacy notices and obtain appropriate consent for data collection and processing.
NFR-41.	The system **SHALL** implement data retention policies in compliance with legal requirements.
NFR-42.	The system **SHALL** support data protection impact assessments (DPIA) for high-risk processing activities.

5.2.4. Security Monitoring and Incident Response

ID	**Requirement**
NFR-43.	The system **SHALL** implement comprehensive logging of security-relevant events.
NFR-44.	The system **SHALL** provide real-time monitoring and alerting for security incidents.
NFR-45.	The system **SHALL** implement intrusion detection and prevention mechanisms.
NFR-46.	The system **SHALL** conduct regular security scans and vulnerability assessments.
NFR-47.	The system **SHALL** have a documented incident response plan for security breaches.
NFR-48.	The system **SHALL** implement rate limiting and other protections against denial-of-service attacks.
NFR-49.	The system **SHALL** provide mechanisms for security patch management and updates.

5.3. Reliability and Availability

5.3.1. Availability

ID	Requirement
NFR-50.	The system **SHALL** maintain 99.5% availability during standard operating hours (8:00 AM to 8:00 PM Palestine time, Sunday through Thursday).
NFR-51.	The system **SHALL** maintain 99.0% availability during non-standard hours.
NFR-52.	The system **SHALL** schedule maintenance windows during periods of lowest expected usage.
NFR-53.	The system **SHALL** provide advance notice of scheduled maintenance to all users.

NFR-54.	The system **SHALL** implement high availability architecture to minimize single points of failure.

5.3.2. Fault Tolerance

ID	Requirement
NFR-55.	The system **SHALL** continue to function with degraded performance in the event of component failures.
NFR-56.	The system **SHALL** implement database replication to prevent data loss in case of database failures.
NFR-57.	The system **SHALL** implement load balancing across multiple servers to distribute traffic and prevent overload.
NFR-58.	The system **SHALL** automatically recover from common failure scenarios without manual intervention.
NFR-59.	The system **SHALL** implement circuit breaker patterns for external service dependencies to prevent cascading failures.

5.3.3. Disaster Recovery

ID	Requirement
NFR-60.	The system **SHALL** maintain regular backups of all data, with full backups at least weekly and incremental backups daily.
NFR-61.	The system **SHALL** store backups in geographically separate locations from the primary system.
NFR-62.	The system **SHALL** define and document Recovery Time Objective (RTO) of 4 hours for critical functions and 24 hours for non-critical functions.
NFR-63.	The system **SHALL** define and document Recovery Point Objective (RPO) of 1 hour, meaning no more than 1 hour of data loss in a disaster scenario.
NFR-64.	The system **SHALL** have a documented and tested disaster recovery plan.
NFR-65.	The system **SHALL** conduct disaster recovery drills at least twice per year.

5.3.4. Error Handling

ID	Requirement
NFR-66.	The system **SHALL** provide meaningful error messages to users without exposing sensitive system information.
NFR-67.	The system **SHALL** log detailed error information for troubleshooting and monitoring.
NFR-68.	The system **SHALL** handle input validation errors gracefully, providing clear feedback to users.
NFR-69.	The system **SHALL** implement appropriate retry mechanisms for transient errors.
NFR-70.	The system **SHALL** maintain system stability when encountering unexpected inputs or conditions.