Recruit Right: Precision Hiring with AI Insight

Project Policy Document

Submitted by,

Muhammad Naeemuddin 1955-2021
Muhammad Abdullah 2206-2021
Muhammad Raza 2207-2021

Supervisor,

Dr. Umer Farooq

In partial fulfilment of the requirements for the degree of
Bachelor of Science in Software Engineering
2025

Faculty of Engineering Sciences and Technology

Hamdard Institute of Engineering and Technology

Hamdard University, Main Campus, Karachi, Pakistan

1. Purpose

This document defines policies governing development, security, quality, deployment, and collaboration to ensure Recruit Right meets high standards of reliability and user satisfaction.

2. Roles and Responsibilities

Role	Responsibilities
Product Owner	Prioritizes features, approves releases, gathers requirements.
Lead Developer	Oversees code quality, reviews pull requests, coordinates releases.
Developers	Write code following standards, create tests, fix bugs.
QA Engineers	Prepare test plans, execute tests, report bugs, verify fixes.

3. Data Privacy and Security

- **Data Minimization:** Only collect necessary data.
- **Encryption:** Store passwords with bcrypt (12 rounds).
- **Authentication:** Google Authentication.
- **Access Control:** Role-based, enforced server-side.
- **Secure Communication:** HTTPS mandatory.
- **Input Validation:** Backend + frontend validation to prevent injections/XSS.
- **Audit Logs:** Log critical actions (login/logout, data changes).
- **Data Backup:** Regular backups with firebase storage.

4. Development and Testing Policy

- Follow coding standards rigorously.
- All code must undergo peer review before merge.
- Maintain minimum 80% test coverage.
- Run regression tests on staging before releases.
- Branching strategy: feature/fix/chore branches only.
- Pull requests must be focused and documented.

5. Deployment and Release Policy

- **Environments:** Dev (local), Staging (auto-deploy from develop), Prod (manual deploy from main).
- **Versioning:** Semantic versioning (vX.Y.Z).
- **Rollback:** Keep stable release available for rollback.
- **Monitoring:** Set up alerts for downtime, errors.
- **Backup:** Automated daily database backups with retention policy.

6. Incident Management

- Detect via monitoring, alerts, or user reports.
- Triage within 30 minutes.
- Hotfix → review → deploy ASAP.
- Communicate incident status to stakeholders.
- Document postmortem within 48 hours.

7. Communication and Collaboration

- Use project management tools (e.g., Jira, Trello) for task tracking.
- Daily/weekly standups to sync progress and blockers.
- Use chat tools (Slack, Teams) for quick communication.
- Keep documentation updated in a shared repository.
- Promote open, respectful communication culture.

8. Accessibility Policy

- Follow WCAG 2.1 guidelines to ensure accessible UI.
- Use semantic HTML and ARIA attributes properly.
- Keyboard navigation and screen reader compatibility mandatory.
- Test accessibility regularly during development cycles.

9. Performance and Scalability

- Optimize queries and API responses for speed.
- Use caching strategies where applicable.
- Conduct load testing before major releases.
- Design system to handle expected user growth gracefully.

10. Backup and Disaster Recovery

- Daily backups of database and essential files.
- Backup copies stored offsite and encrypted.
- Disaster recovery plan tested every 6 months.
- Define RTO (Recovery Time Objective) and RPO (Recovery Point Objective) for critical services.

11. Contribution and Code Quality

- No direct commits to protected branches (main, develop).
- Require at least one review per PR.
- Enforce automated tests and linting before merges.
- Use feature flags for large or risky features.
- Encourage clear, descriptive commit messages.

12. Compliance and Legal

- Obtain user consent for personal data collection.
- Maintain up-to-date Privacy Policy and Terms of Service.
- Use only properly licensed third-party software.
- Adhere to relevant data protection laws (e.g., GDPR if applicable).

13. Review and Update Process

- Review this document every 6 months or after major updates.
- Updates approved by Product Owner and Lead Developer.
- Communicate policy changes to all team members promptly.