**Security Requirements**

**1. Authentication and Authorization:**

* Users must authenticate securely using multi-factor authentication (MFA) to verify their identity.
* Implement role-based access control (RBAC) to restrict access to features and data based on user roles and permissions.

**2. Data Encryption:**

* All data, both in transit and at rest, should be encrypted using strong encryption algorithms (e.g., AES).
* Implement Transport Layer Security (TLS) for secure communication between the app and servers.

**3. Compliance with Data Protection Regulations:**

* Ensure compliance with data protection regulations such as GDPR, HIPAA, or CCPA.
* Implement mechanisms to obtain user consent, provide data access, and enable data deletion upon request.

**4. Secure Data Storage:**

* Utilize secure database configurations and prevent common vulnerabilities like SQL injection.
* Implement data encryption at rest and during backup processes.

**5. API Security:**

* Secure API endpoints with proper authentication mechanisms (e.g., OAuth).
* Implement rate limiting and monitor API usage for suspicious activities.

**6. Secure Code Development:**

* Follow secure coding practices to prevent common vulnerabilities like XSS, CSRF, and injection attacks.
* Regularly update and patch dependencies and libraries.

**7. Regular Security Testing:**

* Conduct security assessments, including penetration testing and code reviews, to identify and remediate vulnerabilities.
* Perform static and dynamic code analysis.

**8. Logging and Monitoring:**

* Implement comprehensive logging of user activities and system events.
* Establish real-time monitoring to detect and respond to security incidents.

**9. Incident Response Plan:**

* Develop a detailed incident response plan outlining steps to take in case of a security breach.
* Ensure clear communication channels and responsibilities for incident resolution.

**10. Data Minimization:** - Collect and retain only the minimum necessary data for the hiring process. - Regularly review and delete unnecessary data.

**11. Third-Party Security:** - Evaluate and vet third-party services and libraries for security vulnerabilities. - Keep third-party components updated with security patches.

**12. Secure AI Models:** - Train AI models on unbiased and representative data to avoid discrimination. - Continuously monitor AI model behavior for potential bias and fairness issues.

**13. Employee Training:** - Train employees on security best practices and conduct regular security awareness programs. - Educate employees about the importance of protecting sensitive data.

**14. Secure Communication:** - Ensure secure communication between the app and external systems using HTTPS and secure protocols. - Regularly update encryption certificates.

**15. Backup and Disaster Recovery:** - Implement regular data backups and a disaster recovery plan to ensure data availability in case of system failures or data breaches.

**16. Secure Deployment:** - Follow secure deployment practices, including server hardening, timely patching, and containerization for isolation.

**17. Legal and Ethical Considerations:** - Ensure AI algorithms avoid bias and discrimination. - Be transparent with users about data usage and processing.

**18. User Education:** - Educate users on security best practices, password management, and recognizing phishing attempts. - Encourage the use of strong, unique passwords.

**19. Regular Security Updates:** - Stay informed about security threats and vulnerabilities and apply updates and patches promptly.

**20. Vendor Security Assessment:** - Assess and monitor the security practices of third-party vendors and service providers involved in the app's ecosystem.