Practical 5

Risk Mitigation, Monitoring, and Management (RMMM) Plan
Project Name: JobLink-Up

1. Technical risks: Technical risks are those that arise from the development process itself. These risks can include compatibility issues with different devices and operating systems, difficulties in integrating various features, or unexpected technical challenges that arise during development.

2. Schedule risks: Schedule risks are those that arise from the project timeline and can include delays due to unforeseen circumstances, such as team member availability, changes in requirements, or technical issues.

3. Budget risks: Budget risks are those that arise from unexpected expenses or cost overruns. These risks can include additional software licenses or hardware upgrades that were not accounted for in the initial budget.

4. Security risks: Security risks are those that arise from vulnerabilities in the software that could compromise the personal information of users.

5. Legal risks: Legal risks are those that arise from potential legal challenges, such as copyright infringement or data privacy violations.

Risks	Mitigation Strategies	Monitoring Procedures	Management Plans
Technical risks	* Conduct regular testing and quality assurance. * Use agile development methodologies. * Work closely with stakeholders and end-users.	* Track progress on testing and quality assurance milestones. * Review code for potential defects. * Obtain feedback from stakeholders and end-users.	* Allocate additional resources for testing and quality assurance. * Adjust the project timeline to allow for additional testing. * Modify the scope of the project to address identified defects.
Schedule risks	* Develop a detailed project plan with milestones and deadlines. * Use project management tools to track progress. * Build in contingency plans for schedule overruns.	* Track progress against milestones and deadlines. * Identify and report potential delays early in the process. * Review the project plan regularly and make adjustments as needed.	* Reallocate resources to critical tasks. * Adjust the project timeline to accommodate delays. * Modify the scope of the project to reduce the amount of work required.
Budget risks	* Develop a detailed budget that includes all anticipated expenses. * Monitor expenses closely throughout the development process. * Build in contingency plans for budget overruns.	* Track expenses against the budget. * Identify and report potential cost overruns early in the process. * Review the budget regularly and make adjustments as needed.	* Seek additional funding. * Adjust the scope of the project to reduce costs. * Renegotiate contracts with vendors.

Security risks	* Implement security measures such as encryption, firewalls, and access controls. * Conduct regular security audits and penetration testing. * Develop a plan for responding to security breaches.	* Review security measures on a regular basis. * Conduct security audits and penetration testing on a regular basis. * Test the security breach plan on a regular basis.	* Hire a security consultant to assist with security measures. * Purchase additional security software or hardware. * Modify the scope of the project to reduce the amount of sensitive data that is collected or stored.
Legal risks	* Conduct a thorough legal review of the software. * Develop a plan for responding to legal challenges. * Obtain legal counsel as needed.	* Review the software for potential legal issues. * Monitor changes in the law that could impact the project. * Obtain legal advice on a regular basis.	* Modify the software to address identified legal issues. * Cease development of the software if necessary. * Obtain insurance to cover potential legal liabilities.