**Risk Management Plan**

**Project Risks**

Members of the team who either permanently or temporarily are unable to participate in the project could result in increased multi-tasking, loss of knowledge, redirection of resources, project delays, and tension within the team. The remaining participants will be assigned the tasks of the inactive member. This is usually not a big problem unless a disproportionate amount of work is assigned to them. The substitute will have difficulty keeping up with the timeline of the project. This is further exacerbated when accounting for the loss of knowledge that makes it difficult for substitutes to pick up where the incomplete task was left on. The substitute will have to dedicate overtime in learning the skills to complete the inactive member’s tasks. If it is something like coding, this is especially difficult as it requires understanding the functions of the current code which may also include a design philosophy different from the substitute method in designing applications. The substitute does have the advantage of asking the original member on how the task is supposed to look like in the end. However, in a scenario where the original member (the coder in this example) is on indefinite leave then the team is faced with the dilemma of whether to preserve the code and struggle to understand it or start over from scratch. Weighing in the cost/benefits analysis is difficult and team members would not appreciate receiving the inactive member’s workload, especially if they are not being compensated for this extra work. The project managers and project planner would need to redesign their plans to accommodate the change. The amount of time and effort it takes to reassign jobs, find the most suitable replacements, and redesign the project plan and project is exhausting. Overall, the mental health and moral among the team would worsen such that it may create tension within the group such as accusations of laziness against each other and perceived unfairness. There is also the possibility of the team inadequately responding to the change which would result in the project being delayed. This would make the organization suffer financial and reputational losses.

Bad project planning is when the team does not take the proper consideration of the requirements of the GUI application, the project timeline to the deadline, and the resources it has. Bad project planning is seen in the initial job delegation where unqualified candidates are chosen. For example, the project planner is out of touch with their other team members. That is, the project planner made did not account the person’s available times to meet up and contact information such as phone number and email. This results in the project planner setting unrealistic target dates for task completion. Strict timelines lead to stressed out workers who do not adequately create and review their output which leads to a badly made product. For example, coders who cannot take the time to thoroughly check their program for any vulnerabilities such as weak authentication. Besides unfulfilled qualifications, incompatible personalities with the job lead to undesirable business practices. For example, the project manager does not like to make social contact. They will not reach out to other members to gather their thoughts on the project and will not set up collaborative efforts between teammates. The lack of research from the project manager makes them out-of-touch with their team and creates a poorly thought out plan that does not account for anybody. It would certainly result in inadequate communications with inconsistent briefing sessions that would inhibit us from achieving objectives in a timely manner. The success of the project will rely on a working environment where people are not accountable for their actions.

The insecurities within the organization and the application encourage attacks from threat agents who are disgruntled members, activists, hackers, and terrorists. One possible insecurity is an ineffective authentication system/policy that contains weak password requirements that make them easily guessable and susceptible to effective brute force attacks. These weak password requirements are seen in the form of unvaried characters, short length, and containing personal identifiable information. The last issue is extremely common among the populace who have insufficient cybersecurity awareness. Insufficient cybersecurity awareness makes people fall victim to phishing, social engineering, and credential stuffing. In phishing, one of our members may receive an email that seems to come from one of our colleagues. However, it is a fraudulent email sent by a threat agent to trick the person into clicking a link and installing malware into their personal device. This would result in the attacker gaining control of the device and stealing the person’s personal information which may include credentials to the application. This allows the threat agent to pose as the victim and social engineer other teammates to give out more information about the application including documentation and code. Team members may feel motivated to reuse credentials from other sites they use but this is a common vulnerability that threat agents hope to exploit. Hackers may attempt to authenticate our application by using stolen credentials obtained from another compromised website. Say one of our members used an Amazon account to make their account on the GUI data processing application. Then Amazon suffered a data breach where attackers stole sensitive data including user credentials which they can test on our application to eventually get in. Other insecurities include the possibility of disgruntled workers sabotaging the project to get revenge or personal gain. Possibly occurring when the person feels they were wronged by the organization by either the workload, voicing their opinions, and deadlines. In the worst case scenario, the attacker may lock everyone else out from server and application.

**Risk Mitigations**

The project manager and project planner should create contingency plans to designate responsibilities of permanently or temporarily inactive members to qualified candidates. Picking the most qualified candidates means interviewing each person about their technical skills and behavioral personalities. Other activities for them to perform is adjusting the timeline of when tasks are worked on, reassigning individuals to tasks, and establishing new working guidelines. Robust guidelines requiring workers to document their work is essential for substitutes to continue progressing the incomplete task. This is especially true in extremely technical tasks such as coding. Programmers are expected to provide enough documentation about their code using snapshots of their output, comments in the script, and a log or checklist that outlines the program’s milestones and errors. To avoid permanent resignations from disgruntled members, the project manager should create a welcoming working environment for the workers. Troubled members of the team should have access to secure and reliable communications to share their struggles about their current workload and contact other members for help. Allowing to share their voices reduces the possibility of these people to feeling isolated from the team and feeling the need to permanently abandon the project.

Creating an effective project plan and project timeline depends on the project planner and project manager researching on the organization. The project planner needs to analyze the project’s objectives, the team’s availability, and the current available resources to create a timeline where workers are given realistic expectations of what needs to be accomplished. The project manager needs to conduct proper interviews that analyzes the person’s character and skill set so that they are assigned to the task they are most likely to succeed in. It also helps asking the person directly what job they want to take. Analyzing this data creates a comprehensive guideline where the team is working efficiently and effectively. The project planner would be able to collaborate with the project manager to create meeting sessions where members are briefed on a variety of topics that includes presenting their findings, assigning new objectives, and sharing feedback on how the project is progressing. Additionally, teammates should be able to socially interact with each other, contribute to the timeline, and place their opinions on setting the daily, weekly, and bi-weekly objectives.

There are physical and digital precautions we can take to prevent security breaches within the project. First is to create strong authentication system for the application. Password requirements must be strict where it encourages users to create them with a greater length and with a variety of characters. However, some professionals in the field even suggest abandoning the current model of the password in favor of a structure of a long passphrase. It reduces the effectiveness of brute force attacks; they are easier to remember than regular passwords; and most major applications can handle up to 127 characters for phrases. Passphrases are recommended to be more than 15 characters long, contain nonsensical and random words, and contain symbols. Additionally, users should avoid using popular phrases and lyrics from songs. Credential stuffing is one of the more preventable attacks to avoid which only requires enforcement of workers creating unique usernames and passwords for the project’s application. Applying multifactor authentication limits successful threat agents who were able to steal the credentials of a team member because they will be blocked by the need of a token. Which can only be obtained through a phone or email account. Team members are trained to understand, identify, and prepare them for phishing and social engineering. When someone needs to change their credentials or ask for information, the team should meet physically in a public area. That would stop any threat agent from social engineering their way into the application. Other important training includes lessons on safely and discretely reporting suspicious activity in the workplace; and lessons on responsible use of organization’s IoT devices. Creating backups of the team’s work minimizes the impact of an accidental or purposeful action of erasing sections or the entirety of the project. This is accomplished by first mandating members to put their work in a shared repository on GitHub. It will contain the project plan, the risk management plan, the earned value sheet, the project management plan, the intelligent GUI application code, the documentation, and the data analysis files. However, active threat agents such as disgruntled team members may still modify their files to make them unreadable or inaccessible. Therefore, two people should oversee creating copies of the shared repository into their private account. These backups are updated on a bi-daily basis since the deadline of the project is on December 1st, 2023. A weekly and a monthly update cycle is not viable.

Employees are trained to understand, identify, and prepare them for phishing and social engineering. Other important training includes lessons on safely and discretely reporting suspicious activity in the workplace; and lessons on responsible use of organization’s IoT devices. Some self-reflection within the organization must be taken to hold perpetrators of cyberattacks accountable. To hold them accountable means to accuse them of misuse of work devices or data. What is considered misuse must be outlined in the code of conduct that outlines the behavior of the workplace. If allowed, organizations publish their investigation of their breach which allows the public to know we are taking privacy seriously.

**Monitor and Incident Response**

Having an incident response plan is essential to strengthening the organization’s cybersecurity. The first step of the plan is preparation, which is establishing a incident response team and gathering the necessary tools to respond to cybersecurity threats. The incident response team is made up of 2-3 members of the team who are hand selected for their greatest knowledge in their field. They will be responsible to monitor devices and network file sharing to find any suspicious activity. This would require deploying software tools such as Wireshark, Nmap, and Burp Suite Pro and anti-virus software. Additionally, using the penetration testing software, Impacket, on our application would help identify vulnerabilities for programmers to patch. Impacket functions as a collection of Python classes for working with network protocols. Impacket focuses on providing low-level access to packets, and for some protocols such as IP, TCP, UDP, ICMP, IGMP, ARP, Ipv4, Ipv6, and ethernet. By using this software, the team gains insights into the scope of the cyberattack, such as knowing affected systems or applications, information about the cause and the origin of the incident, and details of the threat agents that carried it out. Once the incident response team understands what the scope is, they go through the containment phase to limit the damage of the cyberattack. In the context of the project, this means to shut down the program, restrict the access of all shared repositories, and contact all team members to warn a breach is being carried out. The final stage in the incident response plan is to document the entire process to create a report that outlines the perpetrators, group and application vulnerabilities, the type of attack, the organization’s response, and guidelines for security improvements. In a scenario where the perpetrator of the attack is from a deviant among the team, some self-reflection within the organization must be taken to hold these perpetrators accountable. To hold them accountable means to accuse them of misuse of work devices or data. What is considered misuse must be outlined in the code of conduct that outlines the behavior of the workplace. Finally, the organizations should publish their investigation to demonstrate our commitment into data privacy and employee and user safety, and the project’s success.