

Impact Risk	Risk Statement	Response strategy	Objective	Likelihood	Impact	Risk Level
GitHub	Any source code pushed to GitHub could potentially contain information that hackers would find useful when trying to maliciously alter the project. The source files could potentially contain hard-coded login credentials which could allow for data leaks.	Use stronger passwords and usernames than just "admin" or "root", and keep them regularly updated.	Reduce the likelihood of hacking and data leaks.	Medium	High	Medium-to-High
Laptop failure	Laptop could break cause any unsaved files that hadn't been pushed to github to be lost.	Make sure laptop is in a safe and comfortable environment where it is unlikely to break.	Prevent loss of data from damaged laptop.	low	high	low
Incorrect input of code	Sloppiness in coding can lead to incorrect input of data which may not initially be detected but is likely to cause problems down the line.	Keep debugging to try and spot obvious errors and use debugging tools/ unit tests to confirm.	Reduce human element of wrong code input.	medium	high	medium

Bugs	Bugs in the various applications can cause them to stop working as they should.	Ask Anoush.	Reduce bugs in the program with the help of mentors.	high	high	high
Wrong file structure	Incorrect file structure can lead to complications in linking different elements of the project	Ensure files are correctly named and structured.	Ensure correct file structure is adhered to.	medium	high	medium
Saving to the wrong branch in gitbash	Incorrectly saving work to the wrong branch on gitbash can cause code to break.	Double check branch before adding and committing changes.	Avoid saving to incorrect branch on gitbash.	low	Low	low