|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ggitRisk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| Github | Due to github being open source, its is quite easy for hackers to be able to access Github repositories and the source code for your software allowing for them to access data kept | Ensure a regular password change is kept | Reduce the likelihood of hacking and data leaks. | Medium | High | Medium-to-High |
| General Data Handling | Due to the prospect of handling clients data in this program, this is a high threat to malicious entities attempting to access it. | Ensure that software holding user details are only able to be accessed by the users and the admins by setting up accounts with permissions | Create accounts with permissions | High | High | Medium |
| UserError | If Full access is allowed users might be able to delete tables full of data. | Ensure that a password is needed to delete tables | Create accounts with permissions | Medium | High | <edium |
| Cloud Hosting | As the database is being hosted online, it allows more avenues of attack and therefore potential theft of data | Make sure that password of the database is complicated enough to prevent a brute force strategy and possibly put a limit on how many times a password can be entered | Ensure that cloud password is secure | High | Medium | High |
| DatabaseOverfilling | Due to how GCP functions, if a bot filled out infinite amount of data into the sql it would mean the costs of running it would increase exponentially | Ensure that if a certain amount of inputs in a short amount of time then to prevent inputs. | Implement a if stament to prevent user inputs. | low | High | High |