|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| SQL injection attacks | Not defined | Use prepared statement for any database queries | To prevent SQL injection attacks | High | High | High |
| Unauthorized database access | Not defined | Have a strong password for connection to the database. Routinely change the password at least once every month | To prevent unauthorized access to the database | High | High | High |
| System failure | Not defined | Use SonarQube for code quality checks to ensure high code quality | To prevent the system for failing due to poor code | Medium | High | low |
| Data loss | Not defined | Have an on-premise backup solution | In the event that the Google cloud Mysql database is unavailable and the data is lost having an on-premise back will ensure that we have a back up | low | high | low |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| Human error | Not defined | Restrict access and give user permissions | To prevent users without the correct permissions deleting or updating records | medium | medium | medium |
| Unsecure connection | Not defined | Encrypted connections | To make sure all connections to the database are secure and encrypted | medium | medium | medium |