Risk	Assessment	Risk	Impact	Responsibility	Mitigation	Response
Database is attacked and data is breached.	Examples include SQL injection and DoS. Hackers will be able to access and read sensitive data sorted in my database such as emails and passwords.	Low	Medium	Rushab Shah	Avoid the use of dynamic queries within applications. Use of prepared statements with parametrised queries will stop SQL injection. Implement user input validation before that input is passed to the application. Suggest users not to use common passwords they have previously used.	Inform users database has been breached and tell them to change their passwords.
Database accidentally deleted	Someone with access to the database i.e admin could accidently delete the entire database and everything stored within.	Low	Low	Rushab Shah	Regularly create back ups of the data either on a cloud-based service or on another machine. This allows the restoration of deleted data at any time with the most up to date records.	Either recreate all the databases from scratch or force a restore using backups. inform users that their data and subsequent posts have been temporarily deleted.
Privilege abuse	Users may abuse legitimate data access privileges for unauthorised purposes to access data.	Low	Medium		Role based access controls within the application which accurately map required access permissions to job function. Procedures which ensure that when staff change roles, their permissions are updated to reflect this, with those no-longer required being removed.	Response not required.
Cloud server loses connection	If the cloud server we are using goes down due to connection issues, our application will be non-functional.	Low	High	Cloud Provider In our case Google Cloud Platform	Set up multiple cloud instances/virtual machines which will start up automatically in the event of a loss of connection.	Continue to start the primary server up again. And have secondary servers ready with backups of data downloaded and ready to go.