|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the**  **hazard present?**  **Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium**  **L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this Action/to do list/outstanding Person**  **control controls responsible**  **in place?** | | | **Signature and date completed** |
| SQL injection | Y | SQL injection of the database to modify the database and do malicious things for example dropping tables | H | Only allow specific SQL queries to be executed or force add specific things from outside SQL. | No | Protect against SQL injections | Admin | 24/01/2020 |
| Hacking | Y | Malicious intent to get into the database and do unwanted things. | H | Strong Username and Passwords. Not left as root root for example. Inserts for Username and Passwords not storing as plain text | Yes | Null | Admin | 24/01/2020 |
| Accidental  dropping of tables | Y | Drop all would completely destroy the database | M | Sql feature to not allow dropping of all tables | Yes | Add security to protect each table | Admin | 12/02/2020 |
| Loss of code | Y | Losing code would result in total loss of the project. Through user error or natural disaster. | L | Backup code to GitHub | Yes | Null | Admin | 12/02/2020 |

**Com.QA IMS Risk Assessment (List additional hazards, risks and controls particular to your project using this Risk Assessment)**

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible.  **Low Risk (L)** actions should be dealt with as soon as practicable.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the**  **hazard present?**  **Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium**  **L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this Action/to do list/outstanding Person**  **control controls responsible**  **inplace?** | | | **Signature and date completed** |
| Editing code breaking the application | Y | An edit could stop the code working completely | M | Backing up data, using tests to check the code and allow it to be fixed. | Y | Null | User | 12/02/2020 |
| Other people using your computer | Y | The computers all have the same password… Someone could log in and destroy everything. | H | None | Y | Probably sort the password situation. | User | 12/02/2020 |

**Risk Assessment carried out by: Nathan Farnell** 

**Date: 13 / 02 / 2020**

© Alv