|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| Hacking | Y | destruction of data. Customer data being stolen or modified | H | * Creating strong passwords * Not providing them as plain texts | Yes | Null | Admin | 12/02/2020 |
| SQL injection | Y | allow malicious modification of the database | H | Stop specific Sql statements from being executed. So stop commands such as Drop table from being executed | No | Only allow specific Sql queries to be executed | Admin | 12/02/2020 |
| Loss of code | Y | Loss of application | H | Backup the code to github | Yes | Null | Admin | 12/02/2020 |
| Editing code breaking application | Y | Application will be unable to run if codes are broken | L | Have backups and also run tests which identifies which line of codes have problem | 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.

**Risk Assessment carried out by: Blake Ezechi Date: 12 / 02 / 2020** 

© Alv