|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk Asssessment |  |  |  |  |  |  |
| Description | Evaluation | Risk level | Impact | Responsibility | Control Measures | Response |
| Leak of sensitive data from shared device | Could lead to personal information of users’ being leaked. | Low | High | Sheyam Ragupathy | Not completing work from unsecure device or network. Ensure all work is saved and closed after use. | Alert users of potential breach and encourage them to change passwords. |
| VM goes down | Could lead to website going down until issue is resolved. | Low | High | Google Cloud Platform | Create a backup VM. | Apologise for inconvenience to users and get site running again. |
| Hardware damage | Unable to continue progress and potential data loss. | Medium | Medium | Sheyam Ragupathy | Have multiple and regular stores of data such as on Github. | Try to retrieve as much data as possible and source alternative hardware to complete the project. |
| Not meeting deadline | Project failure. | Low | High | Sheyam Ragupathy | Systematic planning and management of project with periodic deadlines. | Ensure additional time is allocated to get back on to deadline schedule if initial sub-deadlines are not met on time. |
| SQL injection attack | Could lead to personal information of users’ being leaked. | Low | High | Sheyam Ragupathy |  | Alert users of potential breach and encourage them to change passwords. |