# Risk Register

This risk register is scale from 1 to 5 for both likelihood of occurrence and impact towards the project. Besides that, the risk register is being separated into five different sub sections to classify them into their respected category of risks. In the risk register, it has risk prevention to show the precaution used to prevent this risk from happening and risk mitigation to show what steps will be taken when this risk happens to prevent further damage to the project.

### Likelihood Scale Description

1. Very low or no chance to occur
2. Low chance to occur
3. Medium chance to occur
4. High chance to occur
5. It will occur in given point of time within the project

### Impact Scale Description

1. Low or no impact towards the project
2. Slight impact but no issues with continuation of project
3. Medium impact and minor problem towards the project
4. High impact and major problem which should be important to fix
5. Catastrophe impact and must be resolve to continue the project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Description** | **Likelihood** | **Impact** | **Risk Prevention** | **Risk Mitigation** |
| **Human Factor** |  |  |  |  |
| Steep learning curve of new programming languages | 4 | 3 | Get to know and improve on the knowledge on the languages used for the projects | Change programming environment back to familiar languages |
| Lack of familiarity on Cloud Computing | 4 | 2 | Research on regarding topic before hand | Get support from team members |
| Lack of support from service providers | 1 | 3 | Not preventable | Get support from user community |
| Loss of team member | 1 | 5 | Constant communication and replacement is prepared | Replace team member |
| **Hardware Issues** |  |  |  |  |
| Hardware failure - Sensor/Beaglebone | 3 | 5 | Stress testing to ensure reliability | Replace hardware with similar or same hardware |
| Cloud computing outage- Electrical failure/system failure | 3 | 5 | Have a backup cloud computing service provider | Redirect traffic to backup cloud computing service provider |
| Compatibility with similar system in case of system environment change | 2 | 4 | Ensure programming languages and hardware used can be used on wide range of devices | Ensure the change has the best compatibility and future proofing |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Description** | **Likelihood** | **Impact** | **Risk Prevention** | **Risk Mitigation** |
| **Security Issues** |  |  |  |  |
| Third Party Intrusion - gaining control of the system | 1 | 5 | Use a reputed cloud computing service provider with enhance security | Terminate any connection to server and retrace intrusion method used |
| Third Party Intrusion - data spoofing/stealing | 1 | 5 | Use a reputed cloud computing service provider with enhance security | Use a better data encryption and transmission method |
| Lack of control over data | 2 | 3 | Limit the amount of user having access over data | Enforce stricter policy regarding the usage of data and who to use it |
| **Legal Issues** |  |  |  |  |
| Location of data center | 1 | 2 | Select the best and closest location based on the users’ location | Choose the next best location for data center |
| Privacy and Legal Agreements | 1 | 5 | Make sure every implementation has been approved legal and compliance with laws and regulation | Edit the system to ensure compliance with law and regulation |
| **Connection/Reading Issues** |  |  |  |  |
| False positive sensor Reading | 3 | 5 | Stress testing to ensure reading are accurate on all circumstances | Revisit programming logic to ensure false positive reading does not occur again |
| Loss of connection between BeagleBone to firebase | 3 | 5 | Have backup connection between BeagleBone to Firebase | Use the next best connection between BeagleBone and firebase |