**Risk Register for Intruder Counter Project**

Date: 28 March 2017

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Risk** | **Description** | **Likelihood** | **Impact** | **Prevention** | **Potential Response** | **Score** |
| R1 | Data Information Disclosure | The program used third party service provider. Hence, the data and information regarding the project and the program can be controlled and accessed by the third party. | 3 | 4 | Choose a reliable, trusted, and well known third party service provider. Make sure to review the privacy agreement with the third party. In addition, keep the data encrypted in the server. | Stop the connection with the third party server and delete all the data in the server database. (make sure to backup the data first) | 12 |
| R2 | Security Attacks and Threats | Cyberattacks is a common thing in the internet. Hence, there is a probability if the attacker bypass the service provider security and threatened the project and data. | 2 | 4 | Always make the data in the database server keep encrypted at all times to prevent from the attackers to access the data. Choose a service provider that has a good background, history and popularity. | Retrieve the data backup and delete the all the data in the server for confidentiality. Use another trustworthy service provider listed in contingency plan for continuing the project. | 8 |
| R3 | Hardware Malfunction | The project requires an IoT kit device hardware as a main requirement. In case that the hardware has a problem or stopped working, the project is also halted until the hardware is fixed. | 1 | 4 | Keep maintaining the hardware condition on regular basis to reduce the risk of malfunction. Use the best quality of hardware for the project. | If the problems on the hardware can be fixed with a short of time, then focus the resources to fix the hardware as soon as possible. If the hardware problems is worse, then use the substitute for the hardware until the original hardware is fixed. | 4 |
| R4 | Server Accessibility and Availability | There would be some cases when the server provider is not accessible by consumer. The reason could be server on maintenance, problems, or cyber attacks. Hence, the program cannot working properly without the server. | 3 | 3 | Prepare a detailed list of contingency plans. The plans consists of other trusted service providers, the list of backup activity and other response action toward risk. | Transfer the connection to use other trusted service provider listed in contingency plans in the time the server is not accessible. | 9 |
| R5 | Resignation of Team Members | Team members is essential to the project. Therefore, missing a team members or developer may result in abandoned project or project failure | 1 | 5 | A regular communication between team members to increase the relationship and trust of team members. | Find any volunteer or other team members outside the project and invite them to the project. If the plan does not worked out, notify stakeholders to move the project to other team or delay the project | 5 |
| R6 | Project Schedule and Time constraint | The project only consist with few members and the project needs to be delivered within delivery date. Therefore, the project may get behind schedule due to lack of resources and unbalanced workload. | 2 | 2 | Review and verify the project scope statement in order for the project to be finished in time with current situation and resources. Create a good quality time management plan for the project. | Respond the problem with backup plans written in contingency plan regarding time management. Inform the client that the project completion date will be delayed. Meeting with the client to discuss any possibilities to fix the problems. | 4 |

**Legends**

Likelihood

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| Minimal Likelihood  0-20% probability for events to occur | Normal Likelihood  21-40% probability for events to occur | Moderate Likelihood  41-60% probability for events to occur | High Likelihood  61-80% probability for events to occur | Very High Likelihood  81-100% probability for events to occur |

Impact

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| Minimal impact. Small or no impact to the project | Normal impact. Impact affecting the project work with reasonable damage. | Moderate impact. Impact has a significant damage toward the project and affecting project progress. | High Impact. Impact has big damage toward the project. May affect the project quality and functionality. | Very High Impact/ Impact has disrupt the project structure and functionality. May result in project failure. |