**Introduction**

AstroDev requires a large security re-hall, this requires implementation of additional security features within different processes to protect the system. The architecture for the software was good for security to be developed on as this is an enclosed system with few systems actually requiring internet. This means that attacks are much rarer than on an open internet.

The plan for this system is to further reduce the chances and impact of any attacks that could occur during the life of this system.

**Scope and Objectives**

The scope of this project will ensure that employees are able to identify different attacks much more easily by implementing training for all employees. Systems will also log employee actions and will use multisystem verification to ensure that data sent is correct and has not been tampered with in any way.

The objectives are:

* To introduce mandatory employee training to identify potential attacks and risks associated with online activities and external interactions.
* To ensure that minimum access privilege is met.
* System activities are logged.
* Only approved IPs can access data.
* Data is encrypted when being sent through a network.
* Access to any of the ship navigation is strictly view only and all other process are automated.

A screenshot of a screen

Description automatically generated**Risk Treatment Plan**

**Software Development Lifecycle Phases with Risk Treatment**

The design phase of the project will take place before the sprints. We will work closely with the AstroDev team to understand any additional design requirements they might need, however we already understand their needs for the backend. This project won’t be development from scratch, rather, we will be using and building on legacy systems to further improve on them. The architecture is already in place and requires strengthening within this project, which we will do so over the course of the development phase.

Development phase:

The development phase of this system will likely be done over the course of a year. This will have to be done modularly as the operations of AstroDev cannot be halted for software and security updates. All systems must not have any integration issues due to the nature of AstroDev, especially the transfer of data from the spacecraft. Rigorous testing must be done before deployment to ensure the safety of the astronauts.

The team will be using TestComplete as an automated testing framework as it supports a wide range of development languages and is able to do functional testing, performance testing, and UI testing which will all play a part in the usage of this software. They will also be using the agile methodology for the development of the software

The development plan will follow CIA for development of software. It will also be done on a closed network within the ground control stations as to prevent any data being intercepted during development.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Dates | Q1 | | | Q2 | | | Q3 | | | Q4 | | |
| Sprints | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec |
| 1 | T01  T02 | | |  |  |  |  |  |  |  |  |  |
| 2 |  |  | T03  T04  T07  T08 | | | |  |  |  |  |  |  |
| 3 |  |  |  |  |  | T05  T06  T09 | | | |  |  |  |
| Testing/ Review |  |  |  |  |  |  |  |  | Review and testing of integration of all sprints and final adjustments | | | |

**Risk monitoring**

Risk monitoring will be done by the IT team and Security Engineer. It is dependent on the type of risk that may occur, however the day to day risks will be handled by the IT team while the Security Engineer will focus on the software based issues.

An automated system will be utilised to check most of the day to day activities and will send an alert to the IT team to check the system. It will send alerts based on a level of severity system from level 1-5 with 5 being the most severe issue.

**Contingency Plans**

Should any of the data be leaked, all people affected will immediately be contacted and given a list of all information that has been leaked. The police will also be notified and no ransom will be paid should the attackers ask for it.

If data tampering occurs, the data be tampered with the system logs in the case of repudiation will be able to show who has changed the data and what piece of data was changed. If the data is changed by an external party through a transmission, the data will be verified by ground control across the different stations. Each station will receive a differe transmission for each piece of data using a different multilayered encryption key.

Should a DOS attack occur, the spacecraft will use star charts to navigate to the destination. If the destination is earth, it will sit in orbit or connect to another space station while waiting for systems to be restored.

In the event of a spoofing attack, the victim will immediately change their password and the password on any other account using the same one.