# CS 405 Project Two Script Template

Complete this template by replacing the bracketed text with the relevant information.

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello everyone. My name is Michael Jones and I am a Developer for Green Pace. Today I will be explaining our new Security Policy. |
| **2** | Here at Green Pace we believe that operating under a Defense in Depth model is the most thorough and sound structure when it comes to security. This allows us to provide many different layers of security to make systems more difficult to infiltrate. |
| **3** | I would like to look at four examples of threats that fall into the categories of likely, priority, low-priority and unlikely. Likely would be a SQL Injection, a very common practice that puts “or” statements into queries to get into systems. Priority would be String Correctness which can overload a string for the number of characters within that string. Low Priority would be Assertions which would validate that a variable is valid when passed into a method. Finally, unlikely is Exceptions which validate values passed into data types to make sure they do not overflow or underflow. While all threats are a concern, we need to prioritize the more likely and higher impact threats. |
| **4** | These are the 10 principles that we need to follow: Validate Input Data, Heed Compiler Warnings, Architect and Design for Security Policies, Keep it Simple, Default Deny, Adhere to the Principle of Least Privilege, Sanitize Data Sent to Other Systems, Practice Defense in Depth, Use Effective QA Techniques and Adopt a Secure Coding Standard. If you would like more information on the individual principles, you can see those in the Security Policy document provided. |
| **5** | Our Coding Standards that we need to adhere to are(listed from most priority to least): Data Type, Data Value, String Correctness, SQL Injection, Memory Protection, Assertions, Exceptions, Divide by Zero, Data Type Casting, and Integer Overflow. If you would like more detailed information about each standard you can reference the handout of the Security Policy document as well. |
| **6** | For Encryption, we must ensure that our data is secure at every stage, in rest, flight and while in use. I believe that having these standards will ensure that our own data, and customer data remains secure at all times. |
| **7** | The “Triple A” policies of Authentication, Authorization and Accounting are laid out in this slide. Authentication to validate a user’s identity such as a form of Two Factor Authentication. Authorization checks the privilege access of the particular to make sure they are allowed to access the particular data, and only at a need to know basis. Accounting checks and validates the statistics for anything that a user does during their sessions. |
| **8** | I was a bit confused for the Unit Testing section. I don’t recall seeing any sample files. |
| **9** | This slide shows the overall automation summary process and how everything should flow from the pre-production phase through production. It remains in a constant loop. |
| **10** | DevSecOps can be summarized as the encompassing tools and infrastructure needed to tie together the pre production and post production stages. They would hand monitoring and implementations of security features. Also they would be in charge of monitoring for attacks, logging checks and anything happening in real-time. |
| **11** | I believe that the best practice strategy for security needs to being implementation at the inception of the project. The biggest risk would be thinking about it too late, or not at all. Also, potentially enforcing not well thought out processes can cause detrimental after effects to the application and potentially the company overall. |
| **12** | I recommend that we allocate a team to tackle to security issues with this project. That should be their sole purpose within the team. This will allow them to focus on security aspects but also still be able to work collaboratively with the development team. |
| **13** | I think that all of the standards covered need to be implemented at some point, but I think we need to prioritize the higher impact ones laid out in the Security Policy document. After those have been completed, we can move down the priority list. Once all standards are implemented we can shift focus to long term management/maintenance. |
| **14** | No references were used during this presentation. |