# CS 405 Project Two Script Template

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

Antonio Sobalvarro

8/14/2022

Project Two: Security Policy Presentation

YouTube link: <https://youtu.be/OrdhxPc6mWY>

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | This is Antonio Sobalvarro, and this is my Project Two presentation for CS 405 at SNHU. |
| **2** | This slide shows Defense in Depth, which is a defense system made up of multiple security layers designed to protect from attacks. Implementing this defense strategy allows a system to stand even if one or more layers are infiltrated. |
| **3** | This chart demonstrates the assigned levels of priority assigned to threats and the assigned probability that are all used to qualify and quantify outside threats that require attention. It’s a good idea to use these because everyone working on the system can be on the same page. |
| **4** | Here, we see the 10 principles. These are meant to serve as guideposts for developers. |
| **5** | There are many coding standards that can, and should be, implemented in the development process of a program. Here, they are presented from highest to lowest level. Each situation will obviously have its own list. |
| **6** | Slide number 6 shows us the encryption policies. As you can see, they are Encryption in Rest, Encryption in Flight, and Encryption in Use. They’re all important to ensure that data is protected at all times and in all states. |
| **7** | Now, we’re on to the Triple-A Policies, which are Authentication, Authorization, and Accounting. Implementing these three policies helps to allow only the correct users to access the system, thanks to the authentication and authorization process. The third policy, Accounting, helps to monitor users’ activities within the system and ensure deeper safety. |
| **8** | Now we see an example of the results of unit testing. The screenshot shows the results of testing various parameters, such as input character length. Conducting these tests helps to ensure that the program will work as it should and ultimately that the code is secure from outside attacks. |
| **9** | This slide shows the circular automation summary, which, when implemented correctly, enforces the principals and standards mentioned in previous slides. |
| **10** | The DevSecOps pipeline mentioned in this slide refers to development, security, and operation that should be followed to inject security into the code throughout its life cycle. The tools section denotes some external tools that should be used to detect vulnerabilities when they are run properly and frequently on the code. |
| **11** | Risks and benefits exist everywhere and with everything. It’s important to be aware of the risks so that you can prepare for them with anticipation and resolve them as quickly as possible. In this slide, I contrast the risks and benefits of tackling an issue immediately or in the future. I, personally, always prefer to tackle and take down issues early, but again, each situation is unique and sometimes you need to see what an issue evolves into before addressing it. |
| **12** | Slide number twelve simply outlines some recommendations to follow and implement in the future if Green Pace is to continue to grow and be successful. Security should absolutely be a number one concern because it affects so many areas and a company’s reputation is paramount in a market riddled with competition. |
| **13** | It’s imperative to be aware of the dynamic landscape of software security and, if possible, to be one step ahead by continuing to educate yourself and your team. It’s a known fact that it’s impossible to build a 100% secure program, but with the right knowledge and by implementing the right policies and standards, along with the correct levels of protection, you can come as close as possible to the coveted 100%. |
| **14** | We’re now at the end of my power point presentation, thank you for listening, and in the words of Ethel Barrymore, “that’s all there is, there isn’t any more.” |