# CS 405 Project Two Script Template

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hi, my name is Chase. Today we will be discussing the new potential security policies for Green Pace. |
| **2** | Here is my explanation of Defense in Depth that also includes this example to go along with it. It shows the different securities and the practices that go with it them to help mitigation. |
| **3** | On this slide I’ve created a threat matrix that shows where each standard falls. It’s a table that is made to clearly show where each standard sits, and the risk associated with it. |
| **4** | I’ve listed the 10 principles on this slide, this is where secure coding should be focusing. Under them, you can see the coding standards which best apply to that principle. |
| **5** | I’ve provided a list of the coding standards and are listed from the highest threat, or most important, to the lowest threat. We can see memory protection is the #1 on the list with the highest threat and assertions being on the bottom of priorities. |
| **6** | These 3 states ensure that all data is covered at all times. At rest, is Encryption that is used to help protect data that is stored on a disk. In Flight, where data is ; finally In Use, where encryption ensures all data is never left unsecured. |
| **7** | Triple-A Framework stands for Authentication, Authorization, and Accounting. Authentication is personal verification, the user, are who you say you are. This can be done using Two Factor Authentication. Authorization is built around permissions, is the person in the able to access what they are trying to? Finally, Accounting, or Auditing, is the process of logging all activities. |
| **8** | Here I’ve provided a screen shot of a unit test that I ran checking the maz\_size |
| **9** | This picture here is DevSecOps pipeline. It’s similar to DevOps but is more focused on securities. We can see the “Verify and Test” section of pre-production, and here is where we will be able to implement our tools to help automate security checks. |
| **10** | There are many tools out there that can help you be successful in testing. Certain tools are needed for certain areas of testing. Astree, Polyspace, Parasoft and CppCheck are some of them that available to devs. |
| **11** | Unfortunately, there will ALWAYS be some sort of risk involved. But always the benefits will out way the risks in this case. The potential of harming customer data should be top priority when thinking about implementing security policies. Cost, prevention, and long term should be a no brainer. |
| **12** | Recommendations are hard, there are many avenues someone can take to help them out. Identifying the gaps in your security is the first hurdle to overcome. Using tools like CppCheck and others to validate written code. Making sure to test early and often. And also, reaching out to a 3rd party company that can test code and/or security. |
| **13** | Creating good practices for the developers to follow is essential to the success of warding off potential attacks. Concepts like Defense in Depth and know the standards are key aspects. |
| **14** | This is the list of references that I used that include articles I used to aid me in this presentation. Thanks for taking the time to listen to me talk about Green Pace’s new policies. |