# CS 405 Project Two Script

**Video:** [**https://youtu.be/E-\_9ziUFtY4**](https://youtu.be/E-_9ziUFtY4)

**Mason Voorhees**

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | HI, I’m Mason and today we will be looking at my security policy presentation. We will be looking over many things to provide a great understanding of how security should look at Green Pace. |
| **2** | Here is an overview of defense in depth. As you can tell, the defense has layers like an onion. Each layer is a different level of security which may be better suited for each type of attack. |
| **3** | Here is the threats matrix where our secure coding standards rank the vulnerability to measure how much each threat has an impact. An impact can be likely with high or low priority and less likely with high or low priority. It just depends on how extreme the vulnerability is. |
| **4** | Here are the ten principles to follow to keep our software secure (read all 10). We heed compiler warnings which means we need to eliminate all warnings. We need to remember to keep everything simple. More cluttered the more likely flaws can occur. WE need to always deny everything unless we get an input we like. Give the least amount of privilege to users to ensure they have less ability to breach the system. Sanitize data so we do not have any issues like SQL injections. Use quality assurance techniques so we are able to test code before releasing it. Adopt a secure coding standard you can follow. And validate input data so all input is in correct format. |
| **5** | Here all the following coding standards. Make sure to follow all these standards to keep your code secure. Not following these standards can cause errors leading to security breaches by attackers. |
| **6** | Here are the encryption policies. We have Encryption in rest, Encryption at flight, and Encryption in use. Each one of these are used in a different situation. Encryption in rest is used to secure data stored on the disk. Kind of like a storage vault. Encryption at flight is used to secure data transferred over the web such as data sent over a remote accessed server or an email. Encryption in use is used to secure data being accessed right now like ram. This is used so when you are looking at contents in a file no one can obtain that information stored in your ram for the time being. |
| **7** | For triple A Policies we have Authentication, Authorization, and Accounting. To explain this easily I will use an example. Say you walk into your company and the security guard needs to look at your badge before you can enter the facility. That would be authentication. Then after that you walk into a room where you need security clearance to enter with a fingerprint scanner that you use and it lets you in, that would be authorization. You look up and see a camera that is watching everything you do and keeps track of the time and what you did. That would be Accounting. Relate this to when someone is accessing information for on a server and it’s the same idea. |
| **8** | In order to keep everything, secure we need to run tests. Unit testing a great way to do this. Unit testing is something that is used early in the development cycle to make sure that everything is secure. This can be used to make sure SQL injection cannot occur, and many other tests to keep everything secure. |
| **9** | Here is a summery of how Automation works, and how both pre-production and production work together to keep software secure. Pre-production is more based around testing the system and making sure everything is working. Production is all about maintaining security and detecting attacks. |
| **10** | Tools used to keep security up to standards would be the DevSecOps pipeline this is a method that allows the development of a project to efficiently keep code secure. The only thing I would suggests to keep in mind is layered security like DiD. Always test during the cycle and not the end of the cycle. This will help detect vulnerabilities early on, so they do not linger on till the end causing bigger issues. |
| **11** | When programming we always have risks. We need to always assume the worst and prepare for it. We need to stay on top of always making sure the security of the system is outstanding. Educating our selves in new ways attacks can be made on a system, allows us to prepare for them ahead of time which will benefit us greatly. |
| **12** | To maintain a secure software, I would recommend   * + - Stay on top of security     - Keep up with new methods attackers use     - Keep everything clean     - Try to make everything simple     - Unit test code     - Don’t wait till the end to test |
| **13** | In Conclusion, the principles and standards mentioned above allows us to conclude what is needed to develop and sustain a secure software development life cycle. We also need to remember that all things outside the company network needs to be treated as classified information to ensure security. |
| **14** | Here are my References. |