# CS 405 Project Two Script Template

<https://www.youtube.com/watch?v=K8_xE12YE3s>

**Mikaylah Blunt**

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello Everybody and welcome to my presentation for Green Pace, I am the developer Mikaylah Blunt and I will be walking you through this |
| **2** | The basis for this policy is basically to showcase at a high level the security risks faced within the organization and standards that can mitigate those issues. Here is an overview that we can go over together. (Read Document) |
| **3** | The table shown is a threat matrix that has the 10 security policies identified in the outline. These have been ranked from likely, unlikely, priority and low priority. |
| **4** | Here we have the 10 principles of security coding; these represent best practices to use in all coding projects. (Read) |
| **5** | Here are the coding standards that are listed within my security policy, I have also put a brief description of what the coding standard is |
| **6** | These are the three encryption states where data needs to be protected, Encryption at rest is encryption that is used to help protect data that is stored on a disk, Encryption in flight is the encryption of data that moves over a network, and In-Use Encryption not only encrypts the underlying data but analyzes data requests in real time and blocks suspicious requests. |
| **7** | Triple-A Framework stands for Authentication, Authorization, and Accounting. Authentication is the process of identifying a user and granting them access to the network, after authentication, the authorization process enforces the network policies, granular access control, and user privileges and Accounting, the final process in the framework, is all about measuring what's happening within the network. |
| **8** | These are some of the unit tests I ran during my testing, you can see successful outputs for both the IsNegativeOutOfRange one, and CustomTestSizeAfterPush |
| **9** | DevOps automation scripts are the tools used to automate the DevOps processes, allowing developers to focus on their core tasks and speed up software delivery. These automation scripts ensure fast testing and deployment of the software in a consistent, reliable, and repeatable way. Looking into the verify and testing phase, you can implement many automation tools. Monitor and detecting can have automatic alerts, which can help notify when problems occur. |
| **10** | Here can see a brief overview of the DevSecOps pipeline, and a further explanation which you can see. A DevOps pipeline is a set of automated processes and tools that allows both developers and operations professionals to work cohesively to build and deploy code to a production environment and here we have some examples of automation tools. |
| **11** | Dont leave security until the end, security is one of the top priorities when it comes to coding and we all must implement them within the process. (read slide) |
| **12** | Some recommendations I can provide would be,  Standardized code ensures readability and consistency.  Continual updates are necessary to address threats and vulnerabilities  Documented policies are essential  Enforcement for each document, policy, and phase. |
| **13** | To wrap this up, some of my closing words would be security is everyone’s responsibility, testing often will help detect vulnerabilities early on within the process as we should remember to be agile. Focus on the defense in depth policy and again with testing we should continually monitor the code. |
| **14** | Thank you for your time, and listening to this presentation and I hope you implement the security measures in the future. |