# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello everybody! My name is Hanah Deering and today, I will be highlighting the key points from the new Security Policy written for and being implemented at Green Pace. |
| **2** | To standardize principles and coding standards across all employees at Green Pace, this security policy was introduced. It follows the best security practices such as Defense in Depth and the Triple-A Framework. Consistence approaches and methodologies for software development at Green Pace requires consistent implementations of the principles outline in the Green Pace security policy to all developed applications. Mitigating commonly faced security flaws early in the development process ensure the digital safety of our company and customers. |
| **3** | We see the threat matrix concerning the ten security policies. You can see that the largest security threats that we will face will come from string and memory management, especially in C++ applications. Automated tools can be used to detect these issues, even the unlikely ones. |
| **4** | There are at minimum ten secure coding principles that we should be focused on here at Green Pace. Under some the principles, you can see the coding standards that best apply to the corresponding principle. All principles are not matched with a certain single standard, they collectively represent the best practices that should be follow by everybody here at Green Pace for coding projects. |
| **5** | Here we see the ten coding standards that are labeled and organized by the level of threat they each pose. The threat level summarizes the severity of the consequences if the standard is NOT implemented. We can also see the likelihood that an exploitable vulnerability will occur if the standard is not implemented, and the expense associated with complying with the standard. String and memory management are at the top of the list since they tend to cause the most frequent and long-lasting damage to systems. |
| **6** | Here we see the encryption policies, or all three states in which data needs to be protected throughout a system. This means that all data will be always protected. First we see at rest, where even though data is not being used, the data that is stored on the disk is still encrypted, making sure that the attacker cannot defeat the encryption to access and read the database. Then we see at flight, or in transit. This is where the data is being sent to or from the system. This includes both internal and external transfers. Encrypting this data adds a layer of protection to the data. Lastly, we see in use. This means where data is being used by the system. The data can be used by the system to either display what the user needs or can be used to verify user accounts. |
| **7** | The Triple-A Framework entails Authentication, Authorization, and Accounting. Authentication is the who are you? Authentication can include user logins like a username and password combination for the user to be able to access the system. Authorization is what can you use? This can include admins or users, in which permissions differ based off the access level. Some users can make changes to the database or includes addition of new users. Accounting is what happened and when did it happen? This refers to records, or log files, which detail things like user logins; new user profile creations; file access events; database updates; data transfers or access. All actions are date and timestamped as a record of occurrence. Usage information can track events such as authorization or resource utilization which can be used in turn for system wide planning. Accounting tracks who are doing what at all times. |
| **8** | Here we can see a couple of screen shots of a unit test that was ran that tested the memory-management functionality of a container. This was coded in C++. Google’s Unit Test framework and the test was passed. |
| **9** | We use automation to enforce and compliance to the standards previously defined. This is the DevOps pipeline. DevOps ends up transforming to DevSecOps by integrating security measures into each step of the DevOps toolchain. In the pre-production phases, threat modeling and security tool training are added into the “Access and Plan” phase. In both the “Design” and “Build” phases, IDE security concerns are addressed. Automation will use several external tools to check for security vulnerabilities, dependency checks, and policy compliance. |
| **10** | Here are some examples of the tools that are recommended. Automation such as Clang and Astree are some of tool that we will be using to address and detect vulnerabilities within the code bases. |
| **11** | With technology constantly evolving, the security of code is no longer just an option - but rather needs to be top priority! There is a war going on right now, in the IT world, between hackers and coders. There are huge benefits to testing often and testing early and the benefits far outweigh the negative consequences of neglecting compliance with this security policy we have enforced here at Green Pace. It is mandatory to implement the best security practices at all times. |
| **12** | Encryption should be everywhere! Unprotected and unencrypted data is too easy to steal. It is like leaving your wallet unattended in a room full of thieves. Lack of encryption is huge mistake made by companies that often ends up costing them in the long run. Secure coding is not a one and done practice, however an ongoing practice of all systems because the threats of today are not always the threats of tomorrow. The cost of protection pales in comparison to the risk of exploitation. |
| **13** | Taking the extra steps from the start, implementing Defense in Depth, and incorporating security testing into everyday practice will allow DevOps to be transformed into DevSecOps here at Green Pace. Adopting all standards to improve the security of systems and applications, is a must. |
| **14** | Thank you for your time and I look forward to seeing improvement through the implementation of this security policy here at Green Pace! |