# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Greene Pace Security Policy cover page. |
| **2** | Overview  The policy that is most important is training. It is important to keep all employees aware of possible threats and follow other policies. |
| **3** | Threats Matrix  Having different threat levels help with prioritizing multiple threats and which need to be attacked |
| **4** | Principles  1. Validate Input Data  2. Heed Compiler Warnings  3. Architect and Design for Security Policies.  4. Keep it Simple  5. Default Deny  6. Adhere to the Principle of Least Privilege  7. Sanitize Data Sent to Other Systems  8. Practice Defense in Depth  9. Security Techniques  10. Coding standards being followed. |
| **5** | Coding Standards   * It checks to make sure that data coming from untrusted sources are safe. * Helps detect security warnings when modifying code and if it is unsafe and at what level it is * To enforce security policies that are designed by us. * Keeping code simple to avoid errors and security risks. * To deny access to users’ permits. * To keep unauthorized people from accessing data that has a higher security level. * It’s a complex subsystem that keeps hackers from injecting malicious code. * Keeping training up to date will help catch possible attacks. Following layers of security step by step will increase security. * testing phases, independent security reviews, and external security reviews can all lead to more secure systems. * To have a secure coding standard for development in whatever language and platform you are using |
| **6** | Triple-A Policies  Authentication- a process where the user is identified by user login and password information for the user to be able to access parts of the system or use a 2-step authentication or multi-tier authentication.  Authorization - is the level of access that a user has within the system.  Accounting -is the process of monitoring what a user is and will keep track of what doing. |
| **7** | Unit testing  Unit testing is to ensure that we have secure functioning code. It tests the code in smaller units which helps pinpoint issues faster. |
| **8** | Automation summary |
| **9** | Tools   * + [Explain the DevSecOps pipeline.]DevSecOps pipeline is an advanced security practice that scans threats and is intelligent.   + Steps are to plan, build, test, release and deploy. |
| **10** | [Insert text.] |
| **11** | Risks and Benefits   * The strategy is lacking the authentication process. |
| **12** | * Gaps in the policies are threats being detected in time and how fast it is fixed. * Lack of monitoring. |
| **13** | **Protecting Secrets and Data**: Secure coding protects against secrets and business data from leaking into the public domain. |
| **References** | * Provide APA-style references with links to resources, articles, and videos that you used in your presentation.] * <https://www.youtube.com/watch?v=-Why_ZjJUhg> * [What Is Zero Trust Security?](https://www.youtube.com/watch?v=d-Jk3GzjwlM) * : [A Practical Guide to Zero-Trust Security](https://threatpost.com/practical-guide-zero-trust-security/151912/) |