# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Welcome, My name is Emmanuel Nieves, This is my presentation where I will present Green Pace’s Security policy. |
| **2** | To start off we have a...  Visual model that helps present a perspective of Defense in Depth. This model illustrates a variety of methods used in cyber security to defend systems and data from intruders. Defense in depth is important because it provides multiple layers of security measures to protect against potential threats or attacks. By using this visual aid we are able to analyze each layer of security and build upon a design that helps ensure that various layers of security exist and that there will always be a security measure in place to prevent a successful attack. This approach helps to minimize the risk of a security breach and mitigates the potential damage if one does occur. |
| **3** | With Secure Coding Standards come certain levels of vulnerability that are measured by the severity and probability of the event occurring. Here we see that half the threats are likely to occur with most of the same threats being of high severity. This Risk analysis matrix helps illustrate the priority each standard holds. |
| **4** | Here we have the 10 Core Security 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. Use Effective Quality Assurance Techniques 10. Adopt a Secure Coding Standard |
| **5** | For the Ten Coding standards for the programming language C++ we have the following:   1. Data Type 2. Data Value 3. String Correctness 4. SQL Injection 5. Memory Protection 6. Assertions 7. Exceptions 8. Input Output 9. Miscellaneous 10. Containers |
| **6** | Encryption in rest - Protects stored data.  Hard drives, phones, computers, cloud assets, etc.  Encryption at flight - Protecting data that is moving.  Devices within a network or moving outside of a network.  Encryption in use - Protects data that is created, edited, or otherwise defined as in-use.  Ensuring protection is in place prior to use. |
| **7** | Authentication - The act of confirming one’s identity.  Ensure a person is who they claim to be.  Authorization - Specifies the access rights and privileges of a user and are an important part of information and computer security.  What a user can and cannot access  Accounting - The process of keeping track of activity while interacting with a system, showing timestamps, accessed resources, and data transfer information.  Bread crumb trail of activity. |
| **8** | Unit testing – Verify and validate components of a program or application, in order to ensure the app will act and respond as intended.  Testing done with Google Test (gtest):  <https://github.com/google/googletest/>  Test to verify if entries is greater than or equal to size |
| **9** | Automation for testing of code should be used as often as possible, it can help keep your development on track if you can utilize a checking process that is automated as opposed to having to create and tailor a test suite yourself every time you write any new code |
| **10** | What is devSecOps?  DevSecOps pipeline is a series of stages that integrate security practices into the software development process. It includes planning, development, testing, deployment, and monitoring. Security is integrated into each stage to ensure secure software development from beginning to end. |
| **11** | Risk and Benefits  Risk of waiting:  Harm to data  Harm to customer trust  Financial cost  Potential future damages of multiple attacks  Benefits of planning:  Mitigating possible damage  Prevent threats  structure and procedure  Reduce possible testing overhead  Example case:  Equifax Breach  Date of case:  March 2017  Result:  Over 143 million users impacted by the data breach, as well as a financial compensation as part of a settlement |
| **12** | Security Policy Essentials:  Policy is a solid foundation. Should be subject to regular reviews and updates, or as gaps are identified.  Annual checks from an outside source, such as a white hat security firm, will help to give security a real-world test and find possible vulnerabilities.  Early application of these policies will help to ensure security is consistently at the forefront of progress. |
| **13** | In conclusion, Adopting best practices and coding standards, defense in depth, and constant consideration to motives that may result in potential attacks attitude towards cyber security throughout development will help Green pace with any future endeavors. |
| **14** | Here we have the list of references |