Joseph Silva Jr.

SNHU

CS 405: 7-1 Project 2: Security Policy Presentation (Script)

12/12/2021

Video Link: <https://youtu.be/wWr1n2tjZvI>

# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | “Hello this is Joseph Silva Jr., and this is my power point for my CS 405 project 2” |
| **2** | “Below is an illustration of the Defense in Depth. Defense in Depth is a multi-layer defense system which uses many programs, features, and IRL defenses to protect a system from an attack. The multi-layer defense allows a system to stay protected regardless of 1 or more of defenses falls from an attack.” |
| **3** | “The table below are certain areas of a threat level table, and these areas are the following: Severity, Likelihood, Remediation Cost, Priority and Level. These threat levels can be found on Confluence to find which standards will have frequent and serious threats.” |
| **4** | “These are the top 10 secure coding practices, and they can also be found on Confluence. On Confluence, the practices are listed and also defined to guide developers during the security features of a project”. |
| **5** | “These are just a few of the standard codes shown on Confluence on ways to protect a system. The listing of these standards has been listed from top to bottom as the highest threat level to the lowest. Also, the threat level table is also displayed to show the areas of the threat level for each standard.” |
| **6** | “This slide lists the different types of encryptions”  “First, the Flight type of encryption is when data is encrypted while being transmitted. The data may not be encrypted while its being stored and/or being used, but the data will become encrypted as its being transferred to another storage location. This encryption protects sensitive data of an entity even if the data is intercepted by an outside source because the data will also be encrypted without the proper key. These encryptions are helpful when employees and/or users are allowed to telecommute or mobile work from the office.”  “Next, the at rest type of encryption is when data is encrypted while it is being stored. The data is accessible, but the encryption prevents the data from being readable without a proper key. This encryption allows a company and/or government to stay protected and have additional defenses against any in-person crimes such as theft of device or thumb drives with sensitive data on it.”  “Last, the In Use type of encryption is when data is encrypted while being used and gives certain users certain access to the data depending on an employee’s security level. This encryption protects the business or government’s databases by creating layers of security to separate user activity from employees. These encryptions prevent new or lower security level employees from gaining total access to the data in the system.” |
| **7** | “These are the types of Triple A policies”  “First Policy will be Authentication and Authentication policy uses User Logins, passcodes, possible secure networks, and other security features such as the use of fingerprint scanning and two-feature identification programs to gain access to a system.”  “Second policy will be Authorization and Authorization policy uses the authentication features to identify the level of security access given to a certain user. The security level allows the user to have admin credentials in order to gain access to databases, files, and employee records. An admin user can make changes to databases and files. Also, admin users also are given the ability to add new users to have access to certain files in the system. “  “Last policy will be Accounting, and Accounting policy uses the features from authentication and authorization to keep records on when data has been changed in a system and who made these changes. There are also certain systems that require a user to make a comment explaining why a user made certain changes to a system. These comments are created for both security reasons and future assistance. These defenses work together in order to give a system a multi-layer defense by the features relying on each other.” |
| **8** | “The following four slides will be examples and questions of different Unit tests on areas of code.  First, Is Capacity Greater than or Equal to size for entries?” |
| **9** | “Second, Does resizing increase collection?” |
| **10** | “Third, Does resizing decrease collection?” |
| **11** | “Last, Is max size greater than or equal for entries?” |
| **12** | “The following is an illustration of an automation security life cycle. Automation will be used for the enforcement of and compliance to the standards defined in a policy.” |
| **13** | “Tools,  First DevSecOps or development, security, and operation, DevSecOps is integrating security into your software development’s life cycle. The software development’s life cycle is the code’s life cycle from its creation to its testing to its push into the main branch”  “Next, External tools such as cppchecker and IDEs testing are used to discover warnings, errors, and messages when developed code is being executed.” |
| **14** | “There are always risks and benefits of developing security features either now or later when developing a project. In our readings, we learned it was not a good idea to leave security development at the end of the project. The following are risks and benefits for the two different time frames during project development.  For now,  Risks are the following: Extended project time length due to multiple tests being conducted on sections of code prior to the sections being pushed into the main project.  Benefits are the following: a more secure project, the entire project’s code is developed and consistent with the consideration of security policies and practices, and security warnings can be discovered during the development phase cycle of the project.  For Wait  Risks are the following: areas of code not compatible with security features, unsecure code during development, cost going overbudget to implement security features at a later time, and timing past due date.  Benefits are a quicker code development phase cycle. |
| **15** | “I recommend projects are developed with security measures being developed in the beginning of the project to have security standards be implemented throughout the entire project. Next, developers need to work as a team, and each need to be held to the same standard of safety and security when it comes to development of a project. After the project development, the triple A and encryption systems can be used at the discretion of the company/individual/government. However, these entities need to stay up-to-date with the latest security features and designs to give their security system the best chance to go toe-to-toe against these attackers their new techniques.” |
| **16** | “Security standards and practices are needed when it comes to the protection and ownership of digital properties. With the world being pushed into a new digital area such as the metaverse, security measures are needed to not only protect a company / government in the future, but the average citizen who will be thrusted into a new reality. In this reality, information and data will be shown and obtained by a new design and value. Security standard and practices will never be 100% guaranteed, but developers and ethical hackers can help systems and projects stay up to date by competing in a form of “chess” with harmful hackers in order to protect these systems in the new digital era of the internet 2.0” |
| **17** | “Thank you for viewing my power point” |