CASEY FARMER

SNHU

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

08/14/2025

Video Link:[7 2 Project Two Presentation](https://www.youtube.com/watch?v=TDfZHGvB0CU&list=PLQR423_TsTo4KCPHuredBbLu1Aq-fkVRB)

[](https://www.youtube.com/watch?v=TDfZHGvB0CU&list=PLQR423_TsTo4KCPHuredBbLu1Aq-fkVRB)

# 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 **Casey Farmer**, and this is my PowerPoint for my CS 405 Project 2.” |
| **2** | Defense in Depth is a multi-layer defense system that utilizes various programs, features, and IRL defenses to protect a system from attacks, ensuring protection regardless of the fall of one or more defenses. |
| **3** | The threat level table on Confluence includes Severity, Likelihood, Remediation Cost, Priority, and Level, which help identify which standards are most likely to face frequent and severe threats. |
| **4** | The top 10 secure coding practices, listed and defined on Confluence, are essential for developers to ensure the security features of a project. |
| **5** | Confluence displays various standard codes for system protection, listed from highest to lowest threat level. The threat level table displays areas of threat for each standard, ensuring a comprehensive view of system security measures. |
| **6** | This slide outlines different types of encryptions, including Flight type, at rest type, and In Use type. Flight type encryption is used when data is encrypted while being transmitted, protecting sensitive information even if intercepted by an outside source. It is useful for telecommuting or mobile work. At rest type encryption is used when data is stored, preventing readable access without a proper key. This helps protect against in-person crimes like theft of devices or thumb drives with sensitive data. In Use type encryption is used when data is encrypted while being used, granting access to specific users based on an employee's security level. This protects databases by creating layers of security to separate user activity from employees, preventing new or lower security level employees from gaining total access to the system. |
| **7** | Triple A policies consist of two types: Authentication and Authorization. Authentication uses user logins, passcodes, secure networks, and security features like fingerprint scanning and two-feature identification programs to gain access to a system. Authorization uses these features to determine the level of security access given to a certain user. |
| **8** | The slides will provide examples and questions for various unit tests on code areas, including determining if the capacity is greater than or equal to the size of the entries. |
| **9** | The question is whether resizing increases collection. |
| **10** | Resizing decreases collection. |
| **11** | Maximum size for entries is greater than or equal. |
| **12** | The security life cycle of automation involves the use of technology to enforce and comply with policy standards. |
| **13** | DevSecOps integrates security into software development's life cycle, from creation to testing and push into the main branch. Tools like cppchecker and IDEs testing help discover warnings, errors, and messages during code execution, ensuring the security of the code throughout its life cycle. |
| **14** | The development of security features in a project involves both risks and benefits. Risks include extended project time due to multiple tests on code sections before being pushed into the main project. Benefits include a more secure project, consistent code with security policies and practices, and the discovery of security warnings during the development phase. Wait risks include areas not compatible with security features, unsecure code during development, overbudget for security features, and timing past the due date. On the other hand, benefits include a quicker code development phase cycle. It is essential to consider both risks and benefits when developing a project. |
| **15** | While suggests on projects should be developed with security measures implemented from the start, ensuring a consistent standard of safety and security. Developers should work together to maintain the same safety standards throughout the project. After development, triple A and encryption systems can be used at the discretion of the company, individual, or government, but they must stay updated with the latest security features and designs to protect against new attackers. |
| **16** | Security standards and practices are crucial for protecting digital properties in the metaverse, a new digital era where information and data are obtained through new design and value. While security standards and practices cannot be guaranteed, developers and ethical hackers can help systems stay updated by competing in a form of "chess" with harmful hackers. This competition helps protect systems in the new digital era of the internet 2.0, ensuring the protection of both companies and citizens. |
| **17** | “Thank you” |