# CS 405 Project Two Script Template

Gavin M. Bish

February 18th, 2025

Project Two: Security Policy Presentation

Link: <https://youtu.be/xJKR-Wp14V0>

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | My name is Gavin Bish and today I will be going over the Green Pace Secure Development Policy |
| **2** | In this presentation, we introduce the security policy of Green Pace, designed to uphold the highest standards of data protection. Our approach integrates defense-in-depth principles, ensuring multiple layers of security to shield our digital assets from emerging threats. This policy is essential for maintaining the integrity and confidentiality of our systems and data across all departments. |
| **3** | The Threats Matrix visualizes the security risks faced by our organization, categorizing them by likelihood and priority. This strategic overview assists in prioritizing responses and aligning our security measures with the most significant threats. |
| **4** | Our security policy is built around ten core principles, each linked to specific coding standards. These principles guide our developers in creating secure software, ensuring that every aspect of security is covered from initial design to final deployment. |
| **5** | We have established ten coding standards that categorize and prioritize vulnerabilities, enhancing our ability to systematically address and mitigate potential risks. Each standard is tailored to confront specific threats, reinforcing our defense-in-depth strategy. |
| **6** | Our encryption policy covers data at rest, in transit, and in use, ensuring comprehensive protection throughout its lifecycle. By encrypting data across all phases, we safeguard against unauthorized access and ensure the confidentiality and integrity of our information. |
| **7** | Authentication, authorization, and accounting (Triple-A) are critical pillars of our security framework. These policies ensure that only authorized users can access specific resources and that all user activities are logged for auditing and compliance purposes. |
| **8** | We employ rigorous unit testing to identify and rectify coding vulnerabilities. These tests include both positive and negative scenarios, ensuring our codebase is robust against various types of attacks. |
| **9** | Automation is pivotal in our security strategy, integrating security practices into our continuous integration and continuous deployment (CI/CD) pipelines. This approach not only enhances efficiency but also ensures consistent enforcement of our security standards. |
| **10** | Our DevSecOps pipeline utilizes a range of external tools to automate and enhance security throughout the software development lifecycle. These tools are crucial for detecting vulnerabilities early and providing the necessary interventions to mitigate risks effectively. |
| **11** | This slide evaluates the potential risks and benefits of our current security strategies. It discusses the urgency of proactive measures versus reactive responses, highlighting where our strategies might be lacking and the potential consequences of inaction. |
| **12** | Based on our ongoing assessments, we identify gaps in our current security policy and recommend measures to address these vulnerabilities, ensuring our defenses evolve in line with emerging threats. |
| **13** | In conclusion, we discuss future standards and practices that need adoption to preemptively address potential security issues, ensuring that Green Pace remains at the forefront of cybersecurity in its industry. |
| **14** | This slide lists all APA-style references, providing credibility and a solid foundation for the data and methodologies used throughout our security policy presentation. |