# CS 405 Project Two Script

Zane M Deso

6/28/2025

Link: [YouTube - Green Pace Security Policy Presentation](https://youtu.be/ir9oiREpToM)

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Welcome to the Green Pace security policy overview. I'm Zane Deso, and this presentation covers our key standards, practices, and recommendations. |
| **2** | Our policy ensures everyone develops with security in mind from the start. This proactive, layered security approach prevents vulnerabilities early. |
| **3** | This matrix ranks each coding vulnerability we identified. It guides us in prioritizing remediation and allocating resources effectively. |
| **4** | These ten principles anchor our security approach, aligning directly with specific coding standards for clarity and actionable guidance. |
| **5** | Our coding standards are ranked strategically, addressing the most severe and likely threats first to effectively reduce risks |
| **6** | Encryption at all levels—rest, transit, and in use—ensures data remains protected even during breaches or attempted interceptions. |
| **7** | Our Triple-A framework guarantees that only authorized users access resources and actions remain traceable and accountable. |
| **8** | Unit testing frameworks integrated into Visual Studio validate code security continuously. These tests automatically highlight vulnerabilities before they reach production. |
| **9** |  |
| **10** | Our automation strategy embeds security checks throughout the entire development lifecycle. This reduces manual errors and enhances overall resilience. |
| **11** | Addressing security now is cost-effective and essential. Delaying security improvements multiplies future risks and expenses. |
| **12** | Our security posture must evolve continually. Regular policy updates, proactive training, and cutting-edge automated tests are essential moving forward. |
| **13** | To prevent future security issues, we need to adopt trusted standards like OWASP ASVS and NIST 800-53 across all workflows. This ensures every layer of the application meets consistent, vetted criteria for security and resilience |
| **14** | These sources informed the structure of our policy, especially NIST’s 800-53 guidelines and OWASP’s ASVS framework. Together, they help ensure our approach is both standardized and up-to-date with the industry’s best practices. |