**8-2 Journal: Portfolio Reflection**

John Schatzl

CS-405-11671-M01 Secure Coding 2025

Prof. Mimi Tam

March 3rd, 2025

Over the length of this course, we’ve delved into key aspects of the Green Pace Security Policy and broader security practices, drawing upon insights gained throughout the course. Integrating security into every facet of the software development lifecycle is crucial, and adopting a secure coding standard is paramount. Rather than relegating security to the final stages, it should be woven into the fabric of the development process. This proactive approach ensures that security considerations are addressed from the outset, minimizing vulnerabilities and fostering a security-conscious development culture. The Green Pace Security Policy emphasizes this by establishing clear coding standards and integrating security checks throughout the DevSecOps pipeline.

Effective risk management involves a thorough evaluation and assessment of potential risks and the cost-benefit analysis of mitigation strategies. This necessitates identifying and prioritizing vulnerabilities based on their severity, likelihood, and potential impact. The Green Pace Security Policy incorporates a risk assessment framework, enabling developers to prioritize remediation efforts based on the threat level of each vulnerability. By carefully weighing the costs and benefits of various mitigation strategies, organizations can make informed decisions to optimize their security investments.

The Zero Trust security model operates on the principle of "never trust, always verify." It mandates strict verification for every user and device attempting to access resources, regardless of their location or network. This approach minimizes the risk of unauthorized access and lateral movement within the network, even if an attacker gains initial access. While the Green Pace Security Policy does not explicitly mention Zero Trust, it aligns with this model by emphasizing strong authentication, authorization, and accounting controls. Implementing multi-factor authentication, role-based access control, and comprehensive logging are steps towards a Zero Trust architecture.

Implementing and maintaining effective security policies requires a multifaceted approach. Clear communication, training, and awareness programs are essential to ensure that all stakeholders understand and adhere to the policy. Regular reviews and updates are necessary to address emerging threats and technologies. The Green Pace Security Policy includes provisions for enforcement, exceptions, distribution, and change control, demonstrating a commitment to ongoing maintenance and improvement.