# 

# CS405 8-2 Journal: Portfolio Reflection

Justin M. Dougherty

justin.dougherty@snhu.edu

Southern New Hampshire University

**Adoption of a Secure Coding Standard and Not Leaving Security to the End**

Adopting a secure coding standard is essential for ensuring a consistent approach to identifying and mitigating vulnerabilities throughout the software development lifecycle. Secure coding standards help developers follow best practices, such as input validation, error handling, and authentication, to reduce risks like SQL injection and buffer overflows. Linford and Company emphasize that security policies, like coding standards, must reflect the organization’s risk appetite and address specific threats, such as social engineering or unauthorized access (Dunham, 2020).

Applying security measures early in the development process prevents costly rework and reduces the risk of exploitation. Delaying security to the end of the development cycle often results in rushed patches or incomplete fixes. By embedding secure coding practices into development workflows, developers can proactively address vulnerabilities, aligning with the principle of "shift-left security."

**Evaluation and Assessment of Risk and Cost-Benefit of Mitigation**

Evaluating risks involves assessing their severity, likelihood, and potential impact on confidentiality, integrity, and availability (CIA triad). For example, implementing multi-factor authentication (MFA) may incur initial costs but mitigates the high risk of unauthorized access. Cost-benefit analyses help prioritize mitigation efforts, ensuring resources focus on addressing the most critical threats.

Security policies also require enforceable risk mitigation strategies. As highlighted in the readings, policies should guide employee behavior and ensure compliance to reduce organizational risk (Dunham, 2020). For instance, policies mandating regular software patching help prevent exploitation of known vulnerabilities, offering a high return on investment in terms of reduced incident costs.

**Zero Trust**

The Zero Trust model transforms security by assuming no user or device is inherently trustworthy, requiring continuous authentication and least privilege access. This approach emphasizes proactive defense mechanisms, such as network micro-segmentation and real-time activity monitoring.

Zero Trust shifts the focus from perimeter security to a data-centric model, protecting assets regardless of their location. As a user, this model enhances security while demanding stricter access protocols. For developers, implementing Zero Trust requires cultural changes and education to highlight the benefits of reduced attack surfaces and improved system resilience.

**Implementation and Recommendations of Security Policies**

Effective security policies, as discussed by Dunham (2020), provide clear guidance on acceptable behavior and practices to safeguard organizational assets. They must be concise, enforceable, and regularly updated to remain relevant to emerging threats. Policies supporting encryption, for example, align with the CIA triad by protecting data during transmission, storage, and use.

Recommendations for enhancing security policies include:

1. **Regular Training**: Equip employees with knowledge of evolving threats, such as phishing and ransomware.
2. **Automation**: Utilize tools like static code analysis and vulnerability scanners to enforce compliance with secure coding standards.
3. **Continuous Improvement**: Review and revise policies annually to incorporate lessons learned from past incidents and adapt to new threats.

**Example for Module Eight Reflection**

An example of a concept for final reflection is the integration of Zero Trust principles into secure coding practices. By treating every access request as a potential threat, developers can design systems that require continuous verification and minimize attack vectors. This proactive approach aligns with secure coding standards and reinforces the importance of addressing security throughout the development process.

**References**

Dunham, R. (2020). *Information Security Policies: Why They Are Important to Your Organization*. Linford & Company. Retrieved from [Linford & Company](https://linfordco.com/blog/information-security-policies/)