**8-2 Journal: Portfolio Reflection**

Noah Coleman

Computer Science, Southern New Hampshire University

CS-405-J8206

Professor Enochson

April 23, 2023

* 1. **Journal: Portfolio Reflection**

**Adoption of a secure coding standard, and not leaving security to the end**

Throughout this course I have learned the importance of secure coding standards, specifically not leaving security to the end. For secure coding to be thorough, it has to be present in every part of production. Code that is written without security, and then has security added, will always be vulnerable to attacks. Code that starts with security as a foundation will be much stronger and more resilient. Having a security mindset will help me to develop more secure code that is better for my employer as well as the consumer.

**Evaluation and assessment of risk and cost benefit of mitigation**

Evaluation and assessment of risk and cost benefit of mitigation is an important part of the secure coding process. By examining potential risks you can analyze what the cost of that risk can be. These costs can range from financial to reputational. Either way, it is typically more cost effective to code trying to prevent a vulnerability rather than take the chance of someone exploiting it. Knowing how much a risk will cost the company can help to persuade upfront development costs in exchange for long term costs during operation.

**Zero trust**

Zero trust is the policy of not trusting any system, and always making devices and users authenticate to gain access. In the modern world where not everything takes place on site, people need to access information from where they are. Because of this every device and every user must be viewed as a potential threat. Following zero trust guidelines allows systems to authenticate users at every step, and avoid as many attacks as possible.

**Implementation and recommendations of security policies**

Implementation and recommendations of security policies is taking the knowledge of secure coding and putting it into practice. Anyone can say that you should strive to create secure code, but without policies in place there is nothing to hold programmers accountable to. Recommendations should be made within a company which should then be turned into policy. These polices should be communicated to everyone in every stage of development.