**Portfolio Reflection**

Jonathan Walton

Southern New Hampshire University

CS-405-T5552 Secure Coding

Mike Prasad

June 25, 2023

The adoption of a secure coding standard is the first step in ensuring that an organization is on the right track in developing code that insists upon the importance of security. A key aspect of any security policy that should be considered for adoption is the idea that security is an ongoing process which retains importance throughout the lifecycle of the development process. By implementing a DevSecOps pipeline that stresses the importance of automation, continuous security, and iterative development, a secure coding policy ensures that developers are held to a standard which requires that security is a key aspect of any application. In addition, by adopting a standard which stresses security’s importance throughout the software development lifecycle, the process of risk-benefit analysis is often lessened by a considerable degree. In effect, by working in compliance with a standard that requires continuous security measures, much of the risk associated with putting security in the latter stages of development is done away with.

Another aspect of consideration when adopting a security policy is the idea of zero trust. Because zero trust is merely a principle, however, it is important that any standard of worth invokes real and robust guidelines for how zero trust should be implemented. One excellent example of a concrete principle by which zero trust can be realized is that of the AAA framework. Under a standard which enforces this framework, developers must ensure that users are continually monitored and evaluated in compliance with the ideas that each user must be authenticated, authorized, and accounted for.

At the end of the day, however, any secure coding standard is only as good as its implementation. The implementation of such a standard is ultimately a question of a company’s culture and the way in which the business is operated. Developers must truly understand and agree with the nature of the policies that they uphold. In order to ensure this, it is critical that all developers are provided with concrete and real-world examples of how leaving security for the end – or lacking zero-trust policies – can affect a product and its reputation.