**8-2 Journal: Portfolio Reflection**

**Mark W. Meyer**

**Southern New Hampshire University**

**CS405-T6652: Secure Coding**

**Prof. Ahlam Alhweiti, M.S**

**August 16, 2022**

When it comes to secure coding, the semantics of code correlates to various endpoints of defense in information security. If care is not taken to validate and authenticate users, privileges, input, output, permissions, and the like, then a security breach could easily expose sensitive information at a great cost to the organization. Thus, adopting a secure coding standard is important because there is a high chance that when using multiple interconnected systems, different languages will be used throughout those systems. So, the absence of secure coding standards can be detrimental to a Defense-in-Depth policy because the more programming languages introduced, the more vulnerabilities there are to be mitigated.

Evaluation and assessment of risk is the backbone of security policy. In other words, mitigating risk is the overarching principle of any Defense-in-Depth policy. It is the very reason developers should not ‘leave security to the end’—because risk can come from anywhere at any point of the software development lifecycle (SDLC). Mitigating risk is the core principle behind zero-trust security policies. The role of defense in depth is to provide an overlapping of multi-layered defense strategies that optimize threat mitigation with a multitude of security checkpoints. Best practice is to implement the Principle of Least Privilege, educate all users including developers and stakeholders, and overall develop a hierarchy of security policies from the perimeter of the building all the way down to the source code.

Implementation of Defense-in-Depth throughout the SDLC is a good example of being proactive and not ‘leaving security to the end’ given the nature of cyber-crime. One good example where this would be effective would be where a newly hired developer—recently educated on the employer’s security policy—is conducting espionage for another organization in trying to put someone on the inside to get privileged information. Principle of Least Privilege would play a key role here in allowing minimal permissions to perform duties.