**8-2 Portfolio Reflection**

Joseph Dugan

University of Southern New Hampshire

CS 405 Secure Coding

Professor Demory

December 16, 2022

Adopting a secure coding standard and not leaving security to the end is essential for implementing a productive developmental approach. Establishing security principles within a developmental team allows for consistency and a standard of reinforcing a secure system. Addressing security in the early stages of development allows for fewer bugs and potential costly remediation at the later stages of a project. Utilizing evaluation of risk and cost benefit of mitigation assessments is essential in determining effective strategies to protect your system while not going over budget. Establishing a ranking system of known security vulnerabilities and priority of remediation will reinforce these efforts. The zero-trust security policy is a network security strategy that adopts the principle that no person or device inside or outside an organizations network should be granted access without authentication. This policy allows protection from previous security gaps where hackers could breach the outside security layers of a network and then have full access once they were inside a network. This policy is extremely effective in providing security especially with the addition of defense in depth security techniques. This hybrid approach of security policies should be adopted to better protect systems and networks. Utilizing these methods will not only promote security but increase productivity within a developmental project.