**Journal: Portfolio Reflection**

William West

Southern New Hampshire University

CS-405: Secure Coding

Aaron Demory

April 23, 2023

Adopting secure coding standards is imperative in establishing a secure system that will withstand many attacks. Leaving security until the end increases the chance that a vulnerability is overlooked and a breach occurs. Figuring out what coding standards are appropriate for the system will take careful designing and planning as well as gathering of requirements from the project owner. Evaluating and assessing risk is a preemptive move that allows developers to build systems that are resilient to breaches as well as efficient in cost. Some implementations might be costly and ultimately unnecessary so it is up to the developer and the project managers to determine what is generally necessary for the security of the system without spending too much time and money on things that are unlikely to be an issue.

Primarily, abiding by the zero-trust policy prevents the system from being accessed by unauthorized persons who might possess malicious motives for the system structure or data. Only users with express permission to access specific areas of the system will be allowed to access those areas. This prevents changes coming from unknown sources as well as makes it easier to track down where changes happen if they need to be modified.

To implement these policies, all company employees must be informed of the policies and encouraged to follow them for the sake of the system’s security. There will also be constant monitoring for unexploited vulnerabilities that must be patched before they are utilized to breach the system.