**8-2 Journal: Portfolio Reflection**

Jehu A. Domenech Ortiz

Department of Computer Sciences, Southern New Hampshire University

CS-405-X6166 Secure Coding 23EW6

Prof. Olga Mill

August 20, 2023

Leaving security to the end leads to the project lacking in security and it being harder to implement. By applying a secure code standard you will program while keeping security in check. These security measures can be further reinforced after the development cycle is done to further improve security.

Depending on the budget for the project sometimes fixing a risk is far too costly for the risk that it brings to the project. If the risk is minor you can leave the problem be and if it needs to be fixed then later down the line if the project gets another fund then the risk can be fixed.

Zero trust is exactly what it sounds like. The system doesn’t trust anybody and measures of authentication and authorization must always be followed some even require continuous validation to prevent somebody from gaining access while nobody is looking.

When implementing security policies looking at what the project needs to focus on should be a top priority. Having too many security policies can water down the focus and make it harder to keep security in check.