Kyle Lund

CS-405

# Portfolio Reflection

## Secure coding Standard

Integrating security at the start of the development cycle is critical to make sure security is not just an afterthought at the end. A secure coding standard are created to prevent security vulnerabilities and help guide developers on how to write their code to keep it as secure as possible. It is also best to adopt a policy early on as fixing security issues later can be costly and damaging to a company.

## Evaluation and Assessment

Risk assessment is an important part of securing a system as it involves identifying any potential threats and vulnerabilities. These threats are then evaluated based on the potential risks and impacts it can have on the program. The cost-benefit analysis is then used to determine if the cost of mitigation is justified by the benefit of reducing the risk. The cost benefit in evaluation and assessment is used to ensure resources are used appropriately and efficiently. An example of this would be to not use a lot of resources and money to mitigate a risk that has a very low probability of occurring and instead use the resources to mitigate higher risk threats.

## Zero Trust

Zero trust is the idea of not trusting any user or developer from the start. This means no one will have unlimited access to the program and will only have access to areas they would only need. No one is automatically trusted with the program and instead approval and verification must take place first before access is granted. This zero-trust policy provides an additional layer of security through verification, multi factor authentication, and least privilege access.

## Implementation and Recommendations

Security policies are the support and structure of a company’s security. They define how issues are to be handled and what is to be expected of the program. A security policy should be clear to follow, enforceable, and align with the companies’ standards. While a security policy may be effective in the present it should be regularly reviewed and checked especially if vulnerabilities are found. Effective security policies are ones that are understood and accepted by all members in the organization. Review and updates should be made to the policy as the threat landscape is always moving and evolving.