**Module Eight Journal**

**Aaron McDonald**

**08/20/2024**

Over the duration of this course we have discussed many different coding best practices and strategies to mitigate the potential of security vulnerabilities. Going through the content of this course, it has become apparent that it is increasingly important to adopt a secure coding standard and to do so towards the beginning of any project that is undertaken. Security is a complex topic that requires many layers of defense to properly employ and with proper planning and preparation from the very beginning, an effective security policy can be created and followed to reduce the likelihood of a security breach.

Leaving security to the end of any project will always leave too much risk at stake, as this will leave any system open to potential attacks and lead to a massive potential loss of business. Customer trust is not something that can be bought and once lost it will likely remain that way forever. Ensuring that any project is secure from the beginning will not only save time and money but will also ensure that customers can trust our business practices with their private information.

Along with security policies, it will be best to utilize a zero-trust policy. This is a policy in which our entire network structure has layers of defense to prevent malicious actors from moving freely within the network. Past business practices would simply have a barrier on the outside of the network, assuming all traffic within the network was safe. However, with the zero-trust policy, we are assuming that no traffic is entirely safe, and we ensure that all traffic is piped through the correct routes of validation. This involves a proxy and a single sign on service that only allows connections to our systems from these services. This ensures that any traffic has been validated as best as possible, a once inside the network the actors cannot move freely without being validated again.

Ultimately, my recommendations for a security policy would be to develop a secure coding standard and to adopt a defense-in-depth strategy. There are far to many layers of security for me to divulge here. Creating a secure coding standard will ensure that any systems we create in-house will remain secure, while creating a defense-in-depth strategy will help to ensure that our network is also secure from the outside world.