Over the course of CS405 Secure Coding we have spent a lot of time understanding the importance of security. One way to integrate is to shift from a DevOps to a DevSecOps to integrate security throughout the entire process of development. This all came together via a security policy that would be a guideline of standards and principles to follow and guide us through the software development process. One of the biggest takeaways was not leaving security to the end as this could cause major setbacks in release timelines with issues that could have been setup correctly from the get-go. The security policy is compromised principles which are built on a foundation of policy, standards, procedures, and guidance.

Understanding what you are taking on is important to properly set yourself up for success. One way of doing this is by performing a risk assessment. A risk assessment is when you take a look at all possible avenues of failure and what needs to be prioritized due to its probability and severity. When one does this due diligence, it can directly translate into savings by preventing unnecessary security issues later down the road, and in theory, when a threat would be harder to fix or spot. It can also be a good way of understanding what risk is worth taking on first for a higher payoff relative to their cost (Seacord, 2013).

Zero trust is a model in which we are strengthening security in the enterprise by trusting no one and verifying everyone (Okta, 2019). This is done by limiting who and when people have access to your applications. The idea of zero adds abstraction to our system in the case someone does can access to our system they then wont have access to everything. This may be a culture shock for some teams but it is an important step to take. Understanding the process over a certain period of time should help others to be willing to adapt.

A security policy is defined as “a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources” (Seacord, 2013). The security policy I created has a couple key pieces to help set a team up for success. It has ten principles which are philosophies and methods we want to follow to keep that security mindset front and center. It also has ten coding standards and will likely get more overtime that can be referred to make sure best practices are followed. These are well defined with links and also have examples of compliant and non-compliant code blocks. It will also give a basic understanding of encryption and triple A defense. These last two pieces are great at giving someone an introduction as to why we want to have this policy and the benefits of it.

**References**

Seacord, R. C. (2013). Secure Coding in C and C. [MBS Direct]. Retrieved from <https://mbsdirect.vitalsource.com/#/books/9780132981972/>

YouTube. (2019). What is Zero Trust Security? Retrieved from https://www.youtube.com/watch?v=d-Jk3GzjwlM.