Robert Lulashi

Southern New Hampshire University

CS 405 6/26/2025

* 1. Journal

Working on the security standards and principles during this course was helpful in understanding the importance of security. Waiting for the end is only asking for trouble because including steps on mitigating breach attempts through adherence to policies such as defense in depth, least privilege, and Triple A. By applying best practices for security measures during the lifecycle of software development, data safety and confidentiality is maintained while decreasing the inherent risks. Mitigating risks throughout development is initially more cost upfront but this cost makes up for potential cost of playing damage control. Security must be addressed throughout development because the risk of what could happen is far greater than minor inconveniences of extra authentication measures or applying a mindset of zero trust.

Zero trust involves verifying on every step for all involved. A user would require more than one login method while admins will need to follow the principle of least privilege. This will only allow the minimum level of authorization thereby reducing mishandling of information. Every step and all personnel must go through extra precautions to reduce risks. It has a core belief that no one is to be trusted and that any attempts of access are of malicious behavior. Applying policies such as defense in depth or zero trust require the help of everyone involved in project development. Regardless of the policy desired, cooperation is required to ensure secure coding is taking place.