**Mohamed. Elmarzougui**

**Southern New Hampshire University**

**CS-405-13497-M01 Secure Coding**

**8-2 Journal Portfolio Reflection**

Don’t leave security to the end” is one of the best practices in software development. It means that security should be integrated into every phase of the Software Development Life Cycle (SDLC), rather than being addressed only after development is complete. This proactive approach helps identify and fix vulnerabilities early, which significantly reduces both risk and long-term costs.

There are many important steps we can take to prevent threats. These include implementing strong access control measures, enforcing multi-factor authentication, and following a Zero Trust policy.

Zero Trust is a security model that requires all users whether inside or outside the network to verify their identity before accessing resources. It operates on the principle of “never trust, always verify,” which helps protect against internal and external threats alike.

In addition, the implementation and regular review of security policies is highly recommended. These policies must be clearly written, consistently applied, and updated as needed to reflect new threats or changes in the system. Clear guidelines help users understand security expectations and ensure that the entire organization is aligned in protecting its digital assets.

By combining secure coding practices, risk assessment, the Zero Trust model, and strong security policies, organizations can build more resilient and trustworthy systems from the ground up.