**8-2 Journal: Portfolio Reflection**

**Jon Wickerd**

**2/28/2025**

From this class I have learned that security should be a priority from the start of software development, not an afterthought. Adopting a secure coding standard helps prevent vulnerabilities early, reducing risks and costs later. Using the best practices like input validation, encryption, and secure authentication strengthens applications and prevents breaches.

Risk assessment and cost-benefit analysis help organizations put security efforts first. Not every risk can be eliminated, so evaluating threats against the cost of fixing the issue ensures the most critical areas get attention. A well-organized approach improves security while maintaining efficiency.

Zero Trust is also a crucial security model that assumes no one is automatically trusted. It enforces continuous verification, least privilege access, and strict authentication. While it may add extra security steps, it significantly reduces attack risks and limits potential damage from breaches.

Security policies establish guidelines for protecting data and systems. Effective policies include access controls, encryption, incident response, and employee training. Regular updates and enforcement ensure they remain effective against evolving threats. Strong policies, along with security-conscious teams, create a safer digital environment.

By integrating security early, assessing risks wisely, adopting Zero Trust, and enforcing strong policies, organizations can protect data, reduce breaches, and maintain user trust.