Artifact Title: CS405 Project One – Security Policy

Enhanced Version: CS405\_SecurityPolicy\_Enhanced

The original artifact was a security policy created for a DevSecOps software company, focusing on secure coding standards. While the original version demonstrated general knowledge of security principles, it lacked real-world technical depth and thorough justification in key areas. To enhance the artifact, I revised three critical standards: SQL Injection (STD-004), Cryptographic Practices (STD-009), and Resource Management (STD-010). These standards were selected for their importance in protecting software systems against common and high-risk vulnerabilities. In each case, I expanded the compliant and noncompliant code examples, clarified the threat assessments, and added specific tooling such as SonarQube, clang-tidy, and Valgrind to demonstrate how enforcement can be automated within modern CI/CD pipelines. I also improved the principle alignment section to clearly map security practices to foundational principles. These updates significantly improve the clarity, accuracy, and practical relevance of the policy. This enhancement demonstrates my ability to design and evaluate secure computing solutions while managing trade-offs and aligning with best practices. It fulfills the software design and engineering outcome by applying professional security strategies in a development lifecycle context.