****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/22/23** | **Elijah Stapleton** |  |

## Client



## Developer

Elijah Stapleton

## Algorithm Cipher

AES-256 is a symmetric block cipher that encrypts data in blocks of 128 bits using a 256-bit key. It is widely used for securing sensitive data, including military, financial, and government communications. AES-256 uses hash functions to provide additional security. These hash functions, such as SHA-256 or SHA-512, take an input message and generate a fixed-length output, known as a hash or message digest. The hash is unique to the input message and cannot be reversed to obtain the original message. The hash functions used in AES-256 are typically used for key derivation, authentication, and digital signatures.

Random numbers are used in AES-256 to generate the initial key and the series of round keys. These random numbers are generated using a cryptographically secure random number generator, which ensures that the numbers are unpredictable and statistically random. The use of random numbers adds an extra layer of security to the cipher.

Symmetric keys, such as the key used in AES-256, are used for both encryption and decryption. Non-symmetric keys, also known as public-key encryption, use two keys: a public key for encryption and a private key for decryption. While symmetric keys are faster and more efficient, non-symmetric keys are more secure and provide additional functionality, such as digital signatures and key exchange.

Encryption algorithms have a long and evolving history, dating back to ancient times when simple substitution ciphers were used. In modern times, encryption algorithms have become increasingly sophisticated, with the development of the Data Encryption Standard (DES) in the 1970s and the Advanced Encryption Standard (AES) in the early 2000s. Currently, encryption algorithms continue to evolve and adapt to the changing needs of cybersecurity, with a focus on efficiency, security, and scalability.

## Certificate Generation Insert a screenshot below of the CER file.Graphical user interface, text, application Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Cannot access Localhost

## Secure Communications

Cannot access Localhost

## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.

Text

Description automatically generated

Text

Description automatically generated

## Functional TestingText Description automatically generatedText Description automatically generated

## Summary

The first layer of security is using the AES-256 hashing algorithm to encrypt plaintext data, the data encrypted was simply my own name however it can be used to encrypt any data such as an SSN, address, email etc. In the case of Artemis Financial it could be user information, business information, financial information etc... The data is secured before it is stored and sent over the internet/ web, all code was viewed for errors and for vulnerabilities before and after refactoring. Another layer of security was using an SSL certificate, this ensures that all communication between a client and server is encrypted and trusted. If a certificate has been tampered with it can be seen by both parties establishing the connection, certificates can be viewed using the “lock” button in any addressed bar on both WebKit and Chromium based browsers. The final layer of security that was implemented was HTTPS, this ensures a secure channel is being used to transmit data over the internet/ web and all sessions must be encrypted to be able to be accessed. If a client does not use the HTTPS protocol then they are not able to access the data stored on the server and vice versa.

## 

## Industry Standard Best Practices

Applying industry standard best practices for secure coding is essential for the overall wellbeing of a company, as it can significantly reduce the risk of security breaches, data loss, and other cybersecurity incidents. Key benefits of implementing secure coding practices are Improved security, Compliance with regulations, Reduced development costs, Competitive advantage. Secure coding practices help to identify and address potential vulnerabilities in software applications, making them less susceptible to attacks. By following industry-standard best practices, developers can ensure that their code is free from common security flaws, such as buffer overflows and injection attacks. Many industries, such as healthcare, finance, and government, are subject to strict regulations regarding data privacy and security; by implementing these practices they can avoid costly fines and legal ramifications. Fixing security vulnerabilities in software applications can be expensive and time-consuming. By addressing potential security issues early in the development process, companies can save money and reduce the overall cost of software development. Lastly a completive advantage can be given to companies that value the security and privacy to their users, they can use this to gain an advantage over companies that sell customer data, do not encrypt customer data, or do not implement industry best standards involving security. Overall, applying industry standard best practices for secure coding is critical for the overall wellbeing of a company. By prioritizing security, companies can reduce the risk of cybersecurity incidents, comply with regulations, enhance their reputation, reduce development costs, and gain a competitive advantage in the marketplace.