****

# 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** | **02/25/2024** | **Ian Viguera** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Ian Viguera

## Algorithm Cipher

Artemis Financial could benefit from an algorithm cipher such as “Sha-256”. This cipher keeps the file encrypted, so it should be protected even if it got illegally accessed. It is, currently, among the safest encryption methods as it encrypts up to 256-bit keys among many applications. Because the cipher relies on Symmetrical keys, it should bear no problem with remote access or export infiltration. Instead, only authorized users will be able to interact with its sensitive data.

## Certificate Generation

A screenshot of a certificate

Description automatically generated



## Deploy Cipher

A close up of a computer screen

Description automatically generated

## Secure Communications

A close up of a computer screen

Description automatically generated

## Secondary Testing

A screenshot of a computer

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated

## Summary

This application executes a secured website connection by encrypting data using “SHA-256” algorithm cipher. “SHA-256” encryption was used due to the protection that offers, especially when exporting data. It ensures that even if the data were stolen or breached, it would still offer layers of encryption protection to secure said data. To add layers of security, multiple dependency checks were conducted to determine possible software vulnerabilities and escapements the application might have. Since some vulnerabilities were false positives, we decided to suppress them to focus only on relevant vulnerabilities. Overall, the application’s code ensures communication between application and security.

## Industry Standard Best Practices

Security and access control are the most important practices to cover on all software applications. Because of this, most of the most common security measures were tested, compared, and considered to apply the most beneficial practice to this specific application. Having a combination of algorithm ciphers and detailed dependency check allows for a breakdown of what areas of the program could be exploited and how they can be protected from them. Having a software environment as protected as this one prevents breaches, unrestricted access, and exploits from attackers.