****

# 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** | **8/24/2025** | **Dalton Gollihue** |  |

## 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

Dalton Gollihue

## Algorithm Cipher

Artemis Financial is going to hold sensitive data in a long-term manner, making the security of such data very important. The algorithm I am going to recommend is the Advance Encryption Standard or AES with its 128-bit key. AES makes a symmetrically generated key by using its random number implementation. This makes it to where there is a single key that the encrypted data is behind. The random number makes it extremely difficult to solve via deduction. AES also has hashing techniques so that the key can be stored and moved into different places to make it much more secure. Encryption has been used since ancient times to hide sensitive information from unwanted parties. It can manifest in the form of different languages, codes, or in any form that can turn information into a code and solved for with a key.

## Certificate Generation

A screen shot of a computer program

AI-generated content may be incorrect.

## Deploy Cipher

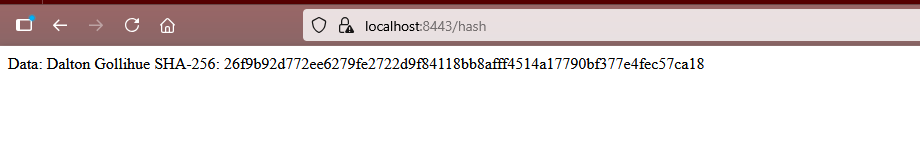
A screenshot of a computer

AI-generated content may be incorrect.

## Secure Communications

A screen shot of a computer screen

AI-generated content may be incorrect.



## Secondary Testing

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

A screen shot of a computer

AI-generated content may be incorrect.

## Summary

First, I started with end-to-end encryption through AES. All of this to help Artemis Financial keep its data safe while its moving through their systems. We also used the Java keytool to make a certificate, to make sure proper devices that are recognized are used. We then use a hash algorithm to get our checksum. We can then update the application.properties file to make sure everything works together. After all of that, we can also utilize the HTTPS protocol with our tools. I also noticed that the version of Maven was out of date, so we updated it. We then suppressed all the false positives in the report.

## Industry Standard Best Practices

I always make sure to leave comments in the code to make sure I can pick it up, and someone can read it after me with no issues. Making sure to update pieces we are using along the way, as well as going through all the false positives in our report, to make sure we aren’t wasting any time.

It’s important to use the best practices for the sake of efficiency. It’s not easy to read code and know what a given developer was thinking. Comments allow for the next developer to see the thought process and work with the previous developer, as opposed to against them.