****

# 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** | **3/3/24** | **Beau Jackson** |  |

## 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

Beau Jackson

## Algorithm Cipher

Taking into consideration of the company Artemis Financials needs I have a recommendation for the best encryption algorithm cipher that would best suit their overall system and cooperation need. The AES-256 encryption would be the best solution to reliable encryption for reliable encryption for long term archive files. This encryption would protect against unauthorized user access, security threats, and data breaches. AES is an encryption that is well regarded for its effectiveness, cryptographic strength, and its ability to secure sensitive data amongst multiple applications.

## Certificate Generation

Insert a screenshot below of the CER file.

[Insert screenshots here.]

## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.

[Insert screenshots here.]

## Secondary Testing

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

A computer screen shot of a program code

Description automatically generated

## Functional Testing

A screen shot of a computer program

Description automatically generated

## Summary

## In the code provided I have assured that the RestController is the secure controller for the endpoint. The SeverController is what is addressing potential vulnerability concerns. In this code I have used SHA – 256 as the cipher and optimize coding with potential attacks in mind.

## Industry Standard Best Practices

To follow industry best practices my recommendation is to continue utilizing the dependency checker once a quarter to access for new vulnerabilities. If there are some established, I recommend utilizing the report to fix them. This way the applications remains secure and up to date.