****

# 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** | **10/14/2023** | **Morgan Getkin** |  |

## 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

Morgan Getkin

## Algorithm Cipher

The encryption algorithm cipher I recommend is the Advanced Encryption Standard (AES). AES is a symmetric key block cipher, which means the same key is used for both encryption and decryption. It is widely recognized as a highly secure and efficient encryption algorithm. AES operates on blocks of data, with key lengths of 128, 192, or 256 bits (typically 128 bits, or 16 bytes). Longer key lengths offer greater security but might be computationally more expensive. It does not directly use hash functions; it focuses on data encryption. However, it can be combined with secure hash functions like SHA-256 for message authentication. Random numbers are crucial for creating secure encryption keys. Proper key management is essential, and the use of strong random number generators for key generation is recommended. AES is a symmetric key encryption algorithm, meaning it uses the same key for both encryption and decryption. It's efficient and suitable for protecting data in transit or at rest. However, secure key exchange mechanisms are vital to ensure confidentiality.

## Certificate Generation

A screenshot of a computer

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications

A screenshot of a computer

Description automatically generated

## Secondary Testing

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

A series of critical security enhancements have been implemented to fortify the Artemis Financial software application. These enhancements encompass certificate generation, cryptographic hash algorithm deployment, and transitioning to HTTPS. Together, these measures contribute to safeguarding sensitive financial data and client information.

Our security approach was guided by the Vulnerability Assessment Process Flow Diagram, a structured methodology for identifying and mitigating vulnerabilities. This comprehensive process ensured that we systematically addressed potential threats and weaknesses. Cryptography, client/server communications, code error, and code quality were a big focus during this implementation due to their relativity for this project.

Security is not a one-size-fits-all solution. To provide comprehensive protection, we adopted a layered security approach. This strategy involved multiple facets, such as secure communication, data integrity checks, and code-level security measures. These layers collectively establish a robust defense against diverse security risks. These security enhancements directly align with risk mitigation. Secure communication, for instance, mitigates the risk of data interception during transit, a crucial aspect in safeguarding sensitive financial information.

Security is an ever-evolving landscape. To address emerging threats and maintain a high level of protection, we recognize the importance of ongoing assessment and updates. Our commitment to continuous improvement underscores our dedication to safeguarding Artemis Financial's software.

Please note that all code files have been attached to this report.

## Industry Standard Best Practices

The security improvements we've made adhere to industry-specific regulations and compliance standards. These measures ensure the application remains compliant with legal requirements, reinforcing trust among clients and stakeholders. Our development team followed established secure coding standards from respected organizations such as OWASP and NIST. These standards provided a solid foundation for identifying and preventing security vulnerabilities at the code level.

Code reviews and rigorous testing were integral components of our security measures. These practices served as proactive gatekeepers, identifying and rectifying potential security issues before they could manifest into critical vulnerabilities. Our team members received comprehensive security awareness training to bolster their understanding of security best practices. Well-informed developers are better equipped to follow security protocols. Security was embedded into every stage of our software development lifecycle. This proactive approach ensures that security is not an afterthought but an integral part of our development process.

We instituted a meticulous patch management process to address security updates and vulnerabilities in third-party libraries and dependencies. Keeping our dependencies up-to-date is paramount in maintaining a secure application. A well-defined incident response plan is in place, outlining procedures in case of a security breach. Being prepared for such contingencies ensures a swift and effective response, minimizing potential damage. Adhering to industry standard best practices for secure coding is not only about safeguarding data but also about upholding the company's reputation and trust among clients and partners. It demonstrates our unwavering commitment to professionalism and reliability. By adhering to these industry standard best practices, we have fortified the security posture of the Artemis Financial software application, ensuring it is resilient against a dynamic threat landscape and positioning the company as a trusted and security-conscious service provider.