Brooke Slampak

CS-305

AES-128 is a great option for keeping Artemis Financials’ long-term archive files secure. It’s a popular and trusted cipher algorithm that scrambles data in a way that makes it basically impossible for hackers to crack. In fact, it is estimated that it would take one billion years to crack AES-128 with a brute force attack! In addition to encryption, best security practices need to be in place to protect against unauthorized access. The biggest risk isn’t actually the encryption itself, it’s how the encryption keys are stored. If they fall into the wrong hands or aren’t properly secured, even the best choice of encryption won’t prevent a breech. That means managing encryption keys properly, using strong authentication, and choosing a secure encryption mode are also integral to maintaining secure archives. In addition, regular security checks and strict access control will go a long way in keeping Artemis Financials’ files secure.

Once employed, AES-128 will be used to encrypt Artemis Financials’ archive files, making sure sensitive financial data stays safe and unreadable to anyone who shouldn’t have access to it. Since AES is a symmetric encryption algorithm, the same key is used to both encrypt and decrypt the files. As stated previously, this makes key security just as important as the encryption itself. A secure system for managing keys will be integral to prevent unauthorized access.

AES-128 meets the security standards required by regulatory bodies like the National Institute of Standards and Technology (NIST), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS), all of which require strong encryption for protecting financial and personal data. Staying compliant means making sure encryption policies are followed, keys are properly managed, and security checks are done regularly. Since AES-128 is compliant with these regulations, Artemis Financial won’t have to worry about falling short of meeting these legal requirements.

While AES-128 is considered highly secure, it’s technically more vulnerable than its biggest contender, AES-256, because of its shorter key length. And while quantum computing could possibly pose a threat to AES-128 in the distant future, for now, it’s still a very effective choice. So why have I chosen AES-128 over AES-256? It offers the right balance of security and performance for this scenario. It’s strong enough for financial and business applications while being faster and more resource-efficient than AES-256, which requires more processing power. While AES-256 provides an extra layer of security, AES-128 is still incredibly tough to crack. With its strong security, speed, and reliability, AES-128 is, in my opinion, the best practical choice for protecting Artemis Financials’ long-term data.

Citations:

* Tobias, E. (2024, October 28). *Zero Trust data-level security and key management*. Ubiq. <https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/>
* Basatwar, G. (2025, March 19). Understanding AES-128 encryption and its significance in the current threat landscape - DoveRunner. *DoveRunner*. Retrieved March 29, 2025, from <https://doverunner.com/blogs/understanding-aes-128-encryption-and-its-significance/>
* Security, T. (2022, December 12). *PCI Compliance Standards (PCI DSS): What you should know and why they matter*. Precisely. https://www.precisely.com/blog/data-security/pci-compliance-standards-pci-dss
* Alder, S. (2025, January 9). *HIPAA Encryption Requirements*. The HIPAA Journal. Retrieved March 29, 2025, from https://www.hipaajournal.com/hipaa-encryption-requirements/#:~:text=The%20HIPAA%20encryption%20standards%20are%20the%20minimum,solutions%20supporting%20AES%20192%2Dbit%20and%20256%2Dbit%20encryption.