The AET

Encryption and Key Management Policy

Purpose and Scope

This Encryption and Key Management Policy provides guidance on the types of devices and media that need to be encrypted, when encryption must be used, the minimum standards of the software used for encryption, and the requirements for generating and managing keys at The AET. Following documented policy will limit mistakes in selecting keys, implementing the encryption/decryption process, and managing keys and other secrets which are common causes of data exposure.

From time to time, The AET may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to The AET including applicable laws and regulations.

This policy applies to all The AET assets utilized by personnel acting on behalf of The AET or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all The AET policies and plans.

Cryptographic Key Requirements

The AET must use industry-approved strong algorithms for encryption processes for data-in-transit and data-at-rest.

Strong Standards

Transport Layer Security
The AET uses strong cryptography and security protocols (TLS 1.2+ or a minimally equivalent protocol) to safeguard sensitive data during transmission over open, public networks. The AET protects the integrity and confidentiality of data passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

The AET prohibits the transmission of unprotected sensitive data using insecure end-user messaging technologies.

Databases at Rest
The AET requires that the encryption of data-at-rest should only include strong encryption methods (AES-256 or a minimally equivalent protocol).

Reference the following for guidance on encryption algorithms: NIST Security Requirements for Cryptographic Modules (FIPS 140-3) and NIST CMVP Approved Security Functions (S.P. 800-140C).

Key Management

- Keys must be protected to prevent unauthorized disclosure and subsequent fraudulent use,
- Users handling private keys must physically and logically secure them,
- Do not share keys with anyone else, and
- Never re-use keys to encrypt other information

Generating Keys

- To generate a key, users must use an industry-standard random key generating mechanism. Reference OWASP Key Management Cheat Sheet for guidance.
- Keys should not be based on common words or phrases.

Key Rotation

Encryption keys should be changed (or rotated) based on a number of different criteria:

- If the key is or may be compromised,
- For example, an ex-employee may have had access to a key.
- After a specified period of time has elapsed (known as the cryptoperiod),
- See Section 5.3 of NIST Recommendation for Key Management for guidance

- After the key has been used to encrypt a specific amount of data, and
- If there is a significant change to the security provided by the algorithm (such as a new attack being announced)

Key Storage

When available, the secure storage mechanisms provided by the operating system, framework or cloud service provider should be used. The key management system must ensure that all encryption keys are secured and there is limited access to The AET personnel.

This may include:

- A physical Hardware Security Module (HSM),
- A virtual HSM, and
- Key vaults such as Amazon KMS or Azure Key Vault

Exceptions

The AET business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other The AET policy. If an exception is needed, The AET management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other The AET policy or procedure may result in disciplinary action, up to and including termination of employment. The AET reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. The AET does not consider conduct in violation of this policy to be within an employee’s or contractor’s course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of The AET as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Roger Hanagriff or a designee is responsible for ensuring compliance across The AET with respect to this policy with the use of a variety of monitoring tools.

The AET reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Roger Hanagriff.

This document was last updated on 01/29/2024.