The AET

Secure Development Policy

Purpose and Scope

The purpose of this document is to define basic rules for secure development of software and systems.

This document is applied to the development and maintenance of all services, architecture, software and systems that make up The AET's product/service.

Users of this document are all employees and applicable contractors who are involved with the development and maintenance of applications and systems at The AET.

Secure Development and Maintenance

Securing the Development Environment

Access to the development environment is restricted only to authorized employees via logical access control. Development and production environments are logically separated.

Secure Engineering Principles

The AET developers follow secure information system engineering practices for the development of new systems and for the maintenance of the existing systems. Minimum-security standards must be maintained and complied with when implementing new systems.

The same secure engineering principles are applied to outsourced development.

All developed code should be reviewed, utilizing the following peer review best practices: https://google.github.io/eng-practices/review/reviewer/.

Security Requirements Related to Public Networks

Roger Hanagriff is responsible for defining security controls related to information in application services passing over public networks:

- the description of authentication systems to be used
- the description of how confidentiality and integrity of information is to be ensured
- the description of how non-repudiation of actions will be ensured

Roger Hanagriff is responsible for defining controls for online transactions, which must include the following:

- how misrouting will be prevented
- how incomplete data transmission will be prevented
- how unauthorized message alteration will be prevented
- how unauthorized message duplication will be prevented
- how unauthorized data disclosure will be prevented

Repository and Version Control

The AET utilizes code version control management tools to track and manage code development, testing, and merges with production. Changes in the development and during the maintenance of the systems must be done according to the Change Management Policy.

Protection of Test Data

Confidential and restricted data, as well as data that can be related to individual persons should not be used as test data, except as required for customer debugging, where approved by customers or where approved by management. On a similar note, test data should be restricted from entering the production environment.

Required Security Training

All engineers must periodically review the OWASP Top 10 as defined in the Change Management Policy.

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 personnel 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

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.