The AET

Network Security Policy

Purpose and Scope

The purpose of this document is to define basic rules and requirements for network security and ensure the protection of information within and across networks and supporting information processing facilities.

This document applies to the security 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 work on network engineering, security, and maintenance at The AET.

Network Controls

The AET manages, controls, and secures its networks, the connected systems, applications, and data-in-transit to safeguard against internal and external threats.

Firewalls & Threat Defense

The AET must utilize network firewalls, web application firewalls, and/or equivalent mechanisms to safeguard applicable internet connections, internal network zones, and applications from threats. The AET configures appropriate firewall alerts and alarms for timely response and investigation. This also applies to applicable wireless networks.

The AET ensures networking ports and protocols are restricted based on the principle of least functionality. Ports and network routes should only be open when there is proper business justification. Firewall configurations and rulesets are maintained. Firewall rules are implemented to minimize exposure to external threats. Significant changes to network services and configurations should be tracked in accordance with the Change Management Policy.

As an additional layer of defense, The AET utilizes monitoring solutions to detect and alert on network-based intrusions and/or threats.

Network Diagramming

Roger Hanagriff maintains network and data flow diagrams. Diagrams are reviewed and updated when significant network infrastructure changes occur.

Network Access Control

In addition to the Network Security Policy, The AET establishes, documents, and reviews the Access Control and Termination Policy based on business and security requirements. This policy also encompasses network access control.

The AET segregates networks based on the required groups of information services, users, and systems.

The AET utilizes firewall configurations to restrict connections between untrusted networks and trusted networks.

Additionally, The AET may utilize security groups and network access control lists (NACLs) to improve network security for individual virtual machines.

Network Engineering

The AET implements security functions in a layered approach, minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

The AET utilizes a defense-in-depth (DiD) architecture to protect the confidentiality, integrity, and availability of information systems and data, i.e. placing information systems that contain sensitive data in an internal network zone, segregated from the DMZ and other untrusted networks.

The AET synchronizes clocks of all applicable information systems to the same time protocol to enforce consistent and accurate timestamping.

Network Service Level Agreements (SLAs)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

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.