The AET

Configuration and Asset Management Policy

Purpose and Scope

This Configuration and Asset Management Policy provides procedures supporting effective organizational asset management, specifically focused on electronic devices within the organization and baseline configurations for The AET assets and systems.

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.

Configuration Standards

Production systems handling confidential data must have documented baseline configurations, when available. The AET management is responsible for following documented standard configurations for all applicable assets including third-party cloud products and employee devices. Configuration standards should be available for reference by applicable personnel.

The AET must continuously harden its systems via Secureframe compliance and security checks as well as Center for Internet Security (CIS) benchmarks and best practices. The compliance checks monitor system security parameters and safeguards.

The AET must regularly patch and keep all applicable systems up to date.

All vendor supplied default configurations, including but not limited to passwords, user accounts, and administrative accounts, should be changed before any systems or devices are implemented.

Each applicable asset and system in the The AET environment should be hardened to the minimum standards defined by The AET management.

Hardening standards should be in line with industry standards and provide sufficient logical and physical security for the asset(s) being configured.

Minimum Device Configuration Settings

The AET devices should be configured to these settings where possible:

- **Encryption:** User endpoint storage is encrypted at rest (e.g. FileVault for MacOS or Bitlocker for Windows)
- **Security Updates**: OS security updates are enforced and monitored
- **Malware Protection**: Malware protection is enabled (e.g XProtect for MacOS, Defender for Windows, or ClamAV for Linux)
- **Screensaver / Lockscreen**: Screensavers / lockscreens are configured to activate after a maximum of 15 minutes
- **Logging**: Logs are captured and stored to assist with security investigations
- **Password Policy**: Required passwords must align with The AET's Access Control and Termination Policy
- **Firewall**: Local firewall is enabled to provide layered host protection unless it interferes with development activities
- **Remote Wipe** (*Optional*):In the event of employee departure or theft, the mobile devices can be remotely wiped

Non-Standard Configuration

If an asset must use a non-standardized configuration, approval of the use must be provided by The AET management and such approval and request must be documented.

Asset Management

The AET inventories and tracks all assets that are used to process, store, transmit, or otherwise impact the confidentiality, integrity, or availability of sensitive information. The asset inventory will include all systems connected to the network and network devices themselves. Examples of items to be inventoried are servers, datastores, network devices, applications, and workstations.

Lost Asset

If an asset is known to be lost or stolen, please report it immediately to .

Acquisition of New Assets

Business considerations must be reviewed, documented, and addressed prior to the acquisition of any new assets. The AET management must approve any new assets that may be used to access The AET data, systems, network, or applications. Reference the Data Classification Policy for more information.

Data as an Asset

Sensitive data is also considered an asset and should be tracked accordingly. Sensitive data must be stored in accordance with all security policies and the location of all covered data regardless of classification or encryption status must be maintained.

Asset Management Procedures

- The AET must maintain an inventory of servers, desktops, laptops, and other devices used to store, create, modify, delete, or transmit confidential information.
- All assets should be mapped to the device’s serial number or another identifier.
- Any asset no longer in use or deemed no longer usable will be removed from the inventory.
- The AET must perform periodic asset management system checks for various classes of asset records.

- Any The AET devices issued to personnel must be returned upon termination or resignation

Asset Inventory Audit

Roger Hanagriff or a designee will be held accountable for the accuracy of the inventory and must perform a documented review of the asset list at least annually.

Physical Media Transfer

Any media or device containing sensitive data must be shipped by a tracked carrier with a recipient signature required. For encrypted data, the encryption key should only be released after the package has arrived and been signed for. Media containing data will be protected against unauthorized access, misuse or corruption during transportation.

Legal advice should be sought to ensure compliance before media containing encrypted information or cryptographic controls are moved across jurisdictional borders.

Asset Disposal

When disposing of any asset, sensitive data must be removed prior to disposal. Any physical media storing confidential or personally identifiable information that is not being repurposed must be destroyed prior to disposal. Sanitization should occur in accordance with the NIST Guidelines for Media Sanitization (NIST S.P. 800-88 Rev. 1).

The AET's third-party providers are responsible for physical protections and disposal of all assets under their control such as databases and servers.

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

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.