The AET

Internal Control Policy

Purpose and Scope

This Internal Control Policy guides The AET regarding the maintenance of an internal control system in order to safeguard the The AET's assets against loss, promote operational efficiency, and encourage adherence to prescribed managerial policies.

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.

Internal Control

Control Environment

The AET senior management recognizes that a proper control environment provides the discipline and structure to help The AET achieve its objectives. The AET manages and maintains its internal controls through the use of the Secureframe platform.

Responsibility

The AET senior management is responsible for ensuring that an adequate and effective internal control system exists at The AET and that dedicated personnel are necessary for monitoring the

performance of the internal control system. Senior management must establish and define responsible parties with accountability for overseeing and maintaining internal control processes and procedures. These lines of accountability should be reviewed annually to ensure that performance measures are being met. Corrective measures or changes in responsibility should be implemented as needed.

Annual Review

Internal control processes and procedures should be reviewed by The AET senior management annually. Senior management may choose to sample a number of controls for review per year. Any outdated or non-operating procedures should be updated or removed. New controls should be implemented where appropriate.

Identified Deficiencies

Identified control failures or deficiencies and proposed corrective action plans for newly identified issues must be addressed and communicated to management.

Evaluation of Internal Controls

- Internal control objectives are identified by relevance to the company, department, business line, or product
- As part of the evaluation process, a review of pertinent policies, procedures, and documentation will be completed to verify that applicable internal controls are operating effectively, and in line with business objectives
- A member of The AET management or a designee will document the review of internal control policies and procedures and sign off on the review. Findings will be shared, as appropriate
- Identified issues are assessed to determine the impact to internal control. If necessary, corrective action plans are developed, tracked via documentation, and monitored until implementation

Changes to Internal Controls

- If a corrective action or change is required, The AET management must assess the changes that could significantly impact the system of internal control including:
- External environment,
- Current business model,
- Leadership, and
- Business relationships (vendors, business partners, and other third-parties)
- All changes must be approved by management before implementation. If the change is related to security of network and IT resources, the change must be approved and documented in accordance with documented change management procedures
- Changes to internal control activities must be communicated to all affected users in a timely manner

Communication with External Third Parties

The AET will communicate with external parties regarding the functioning of internal control (i.e. material changes to internal controls that affect nondisclosure agreement or contractual confidentiality and privacy provisions.).

The AET will conduct an assessment to determine whether changes need to be communicated to and affirmed by the customer, partner, vendor, or other third parties. The manner in which the change is communicated must be in line with the significance of the change.

Communications with legal or regulatory implications must be reviewed and approved by management.

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.