The AET

Vendor Management Policy

Purpose and Scope

This Vendor Management Policy guides The AET in the execution, management, and termination of vendor and other third party agreements. 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 employees and contractors acting on behalf of The AET or accessing its applications, infrastructure, systems or data. All employees and contractors are required to read, accept and follow all The AET policies and plans.

Vendor Management Process

The AET will maintain a profile of all The AET vendors that includes the vendor, their executed agreements, and the appropriate reviews and documentation of such vendors in accordance with this policy. Such reviews will be based on the risk level of each vendor.

In order for The AET to contract with a new vendor, the following steps should be taken in advance:

(1) Request for New Vendor

If an employee or contractor of The AET wishes to use the free or paid services of a new vendor, a request for such use must be submitted to your manager. As part of the submission, the request may include a completed The AET new vendor request form.

(2) Risk Assessment and Due Diligence

Before entering into a contract and granting access to The AET systems, a risk assessment and appropriate due diligence should be performed to determine the possible risk and impact to The AET. Vendors should be separated into three risk tiers: High, Medium and Low. Risk assessments must occur for all high risk vendors.

In particular, a vendor security assessment should include answers to at least the following:

- Is the vendor of a customer-facing nature?
- Would the vendor be involved in receiving and storing confidential data. Examples include: customer data, employee data, regulatory data, or financial data?
- If so, where does the vendor use, access, and store such data?
- What security controls and measures does the vendor have in place?
- Request copies of all relevant security policies.
- Has the vendor undergone third party audits (such as SOC2, HITRUST, ISO)?
- If so, a review of such reports should be performed and identified weaknesses should be documented
- Is there a risk of regulatory scrutiny and customer harm associated with the vendor?
- What is the operational reliance on this vendor?
- Does this vendor present supply chain risk?

(3) Contract Review

A confidentiality agreement or services agreement containing a confidentiality clause or equivalent must be reviewed and executed prior to any use of services and sharing of confidential data between The AET and any third-party.

Vendor agreements should at a minimum require that third-parties maintain the privacy and security of the confidential information stored, used, or disclosed on behalf of The AET.

(4) Monitoring of Vendors

Roger Hanagriff or a designee is responsible for annual or more frequent vendor reviews of high-risk vendors as determined by this policy.

The AET must periodically review all third-party agreements to reasonably ensure that vendors remain in compliance with state and federal law and appropriately address any legal risk to The AET. Agreements will be updated and amended as necessary when business and regulatory requirements change.

Annual reviews of vendors will be documented and retained for audit purposes. The annual review may include the gathering of applicable compliance audits (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, etc.) or other evidence of security compliance including performing a review of in-place security controls.

Results of the reviews must be compared to in-place agreements and/or SLAs to ensure that services are being provided as intended. If vendors are found to be in violation of any executed agreement(s), action plans and processes may be initiated to remedy the issue(s) or access to The AET systems may be removed immediately.

(5) Termination of Vendors

Upon termination of a vendor's services, all confidential information stored by the vendor should be deleted and/or provided back to The AET within 60 days.

(6) Assignment of Vendor Relationship Owners and Contacts

Vendors should be assigned internal relationship owners, and key external vendor contacts should be identified. Vendor contacts should be actively maintained in case any issues with the vendor's product or service arise.

Vendor Security Controls

In order to protect The AET, certain high-risk vendors may require additional controls such as:

- Not to use or further disclose confidential information other than as permitted or required by the agreement or as required by law
- Define the following service levels, where applicable:
- Service definitions,
- Delivery levels,

- Security controls,
- Aspects of service management, and
- Issues of liability, reliability of services, and response times
- Use appropriate safeguards to prevent use or disclosure of confidential information other than as provided for by the agreement
- Employ or implement appropriate administrative, physical, and technical security safeguards and privacy practices that meet the use and disclosure requirements of The AET
- Require a prompt report of any inappropriate use, disclosure or breaches of confidential information
- Breach notification must include the following:
- names of breached individual(s) and contact information,
- date breach occurred and the date breach was discovered,
- information/data that was breached (e.g., social security number, name, address, etc.),
- mitigating activity undertaken to limit damages, and
- security controls that will be implemented to reasonably ensure a similar breach does not occur in the future
- Reasonably ensure that any agents, including subcontractors, who use and disclose confidential information will agree to the same restrictions and conditions that apply to The AET and its team members.
- Require that third-parties coordinate, manage, and communicate changes to any services currently provided that could affect the security, availability, or integrity of covered data.
- Review warranties, indemnification and limitations of liability to determine maximum cost of risk.
- Upon termination of the agreement, if feasible, the service provider or vendor will return or destroy all confidential information, used or disclosed by the service provider on behalf of The AET, in any form and will retain no copies of such information.
- If return or destruction is not feasible, the service provider may extend the agreement's privacy and security protections to confidential information and limit further uses and disclosures to those purposes that make the return or destruction of confidential information infeasible.
- Authorize The AET to terminate the agreement if The AET determines the service provider or vendor has or is violating the executed agreement.

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.