The AET

Security Incident Response Plan

Purpose and Scope

The Security Incident Response Plan provides a systematic incident response process for all Information Security Incident(s) (defined below) that affect any of The AET's information technology systems, network, or data, including The AET data held or services provided by third-party vendors or other service providers. 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 plan 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.

The AET intends for this plan to:

- Define the The AET security incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.
- Assist The AET and any applicable third parties (including vendors and partners) in quickly and efficiently responding to and recovering from different levels of information security incidents.
- Mitigate or minimize the effects of any information security incident on The AET, its customers, employees, and others.
- Help The AET consistently document the actions it takes in response to information security incidents.

“Information Security Incident” means an actual or reasonably suspected unauthorized use, disclosure, acquisition of, access to, corruption of, deletion, or other unauthorized processing of sensitive information that reasonably may compromise the privacy, confidentiality, integrity, or availability of that information.

Management

The AET has a Security Response Team (SRT) consisting of predetermined employees from key departments at The AET to manage security incidents. The SRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to the The AET systems, network, and data; (b) minimize economic, reputational, or other harms to The AET and its customers, employees, contractors and partners; and (c) manage litigation, enforcement, and other risks.

The SRT also oversees and coordinates the development, maintenance and testing of the plan, its distribution, and on-going updates of the plan. The Security Incident Response Plan is activated or enabled when a security incident occurs, and the SRT is responsible for evaluating the situation and responding accordingly. Depending on the severity of an incident the SRT may request engagement from various support teams to assist with the mitigation of the incident. The SRT meets on a periodic basis for training, education, and review of the documented plan.

The SRT consists of a core team with representatives from key The AET groups and stakeholders.

The current SRT roster may be contacted at .

Incident Response Process

The process outlined below should be followed by the appropriate Staff at The AET in the event of an Information Security Incident. The AET shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. The AET shall document each identified Information Security Incident.

Detection and Reporting

Automated Detection

The AET may utilize automated detection means and other technical safeguards to automatically alert The AET of incidents or potential incidents.

Report from The AET Personnel
All The AET personnel must report potential security incidents as follows:

1. If you believe an incident occurred or may occur or may have identified a threat, vulnerability, or other security weakness, please report it to the following email immediately: ;
2. Provide all available information and data regarding the potential incident; and
3. Once an incident has been submitted, please stop using the affected system, or any other potentially affected device until being given the okay from the SRT

Report from External Source
External sources, including The AET's customers, who claim to have information regarding an actual or alleged information security incident should be directed to .

Employees who receive emails or other communications from external sources regarding information security incidents that may affect The AET or others, security vulnerabilities, or related issues should immediately report those communications to and should not interact with the source unless authorized.

Response Procedures

Overview
Responding to a data breach involves the following stages:

1. Verification
2. Assessment
3. Containment and mitigation
4. Post-breach response

All of the steps must be documented in an incident log and/or corrective action plan.

The data breach response is not purely linear, as these stages and the activities associated with these stages frequently overlap. The AET must keep a record of any actions the organization takes in responding to the incident and preserve any evidence that may be relevant to any potential regulatory investigation or litigation including through use of an incident log, corrective action plan or other applicable documentation.

(1) Verification

The SRT will work with The AET employees and contractors to identify the affected systems or hardware (such as a lost laptop or USB drive) and determine the nature of the data maintained in those systems or on the hardware.

The SRT will determine the threshold at which events are declared a security incident and officially initiate the incident response process.

(2) Assessment
Following verification of an Information Security Incident, the SRT will determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to The AET and its customers, employees, or others.

The incident assessment must include what employees or contractors were affected, what customers were affected, and what data was potentially exfiltrated, modified, deleted or compromised.

The SRT will work together to assess a priority with respect to the incident based on factors such as whether:

1. the incident exposed or is reasonably likely to have exposed data; or
2. personally identifiable information was affected and the data elements possibly at risk, such as name or date of birth.

In addition, the SRT will consider whether the disclosure was:

1. internal or external;
2. caused by a company insider or outside actor; and/or
3. the result of a malicious attack or an accident.

Lastly, if an information security breach has occurred, federal/country-wide law enforcement and local law enforcement should be contacted and informed of the breach. Law enforcement should be contacted in alignment with applicable breach notification laws. Internal and/or external general counsel should lead law enforcement communication efforts (in collaboration with SRT). If general counsel is not available, SRT should lead law enforcement communication efforts.

(3) Containment and Mitigation
As soon as The AET has verified and assessed the breach, the SRT must take all necessary steps to contain the incident and return the The AET systems back to their original state and limit further data loss or intrusion.

Such steps may include:

1. Acting to stop the source or entity responsible, for example by:

2. taking affected machines offline;
3. segregating affected systems; or
4. immediately securing the area if the breach involves a physical security breach.
5. Determining whether other systems are under threat of immediate or future danger.
6. Determining whether to implement additional technical measures to contain the data breach, such as changing locks, passwords, administrative rights, access codes, or passwords.

(4) Post-Breach Response
Any post-breach response including external and internal communications, notifications, and further inquiries will depend on the assessment and priority of the data breach.

The AET will respond to confirmed disclosures affecting data subjects in accordance with breach notice periods defined in applicable laws and regulations. In the event of a data breach, if such affected data pertains to an EU citizen, The AET must notify the data subject and necessary authorities within 72 hours.

As part of the final response based on the results of the breach, The AET will review applicable access controls, policies and procedures and determine whether to take any actions to strengthen the organization's information security program.

Key Learnings

As soon as the incident has been resolved, The AET senior management should meet with the SRT and other relevant team members of the The AET for a post-mortem to better understand the incident that took place, and determine how similar incidents may be prevented in the future.

The retrospective should be documented and key learnings from the retrospective should be presented to all appropriate team members in a timely manner.

Testing

Testing the plan annually is critical to ensuring the plan is effective and practical. Any gaps in the plan that are discovered during the testing phase will be addressed by The AET management. All tests must be thoroughly documented.

Testing of this plan may be performed using the following methods:

Walkthroughs
Team members walk through the steps documented in this plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This walkthrough provides the opportunity to review the plan with a larger subset of people, allowing the team to draw upon an increased pool of knowledge and experiences. Team members should be familiar with procedures, equipment, and offsite facilities.

Table Top Exercises
An incident is simulated so normal operations will not be interrupted. Scenarios of various security incidents are used and this plan is put into action to determine its use and effectiveness.

Validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

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

This plan will be reviewed and tested on an annual basis. Ensuring that the plan reflects ongoing changes to resources is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updates; and training personnel. Test results will be documented and signed off by The AET management. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is tested, maintained and enforced by Roger Hanagriff.

This document was last updated on 01/29/2024.