The AET

Vulnerability and Patch Management Policy

Purpose and Scope

This Vulnerability Management Policy defines an approach for vulnerability management to reduce system risks and integrate with patch management. 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.

Vulnerability and Patch Management Program

The AET maintains a vulnerability management process that is integrated into the Change Management Process.

The AET may periodically test the security posture of its applications and systems through third-party testing as well as vulnerability scanning.

The AET also monitors multiple security alert lists such as the CVE Database and US-CERT to get up to date information on the latest vulnerabilities and threats.

Third-Party Penetration and Vulnerability Tests

The AET schedules third party security assessments, penetration tests, and/or dynamic analysis tests at least annually.

The AET periodically performs vulnerability scans.

Identifying Vulnerabilities

The AET reviews third-party penetration test reports and vulnerability scan results to verify vulnerabilities and determine impact.

Scoring Vulnerabilities

Vulnerabilities are derived from the Common Vulnerabilities and Exposures (CVE) Database and are documented and scored based upon the Common Vulnerability Scoring System (CVSS) standard.

Mitigating Vulnerabilities

If remediation is required, the appropriate team member at The AET will be notified of the requirements to remediate or mitigate the vulnerability and the time frame of such requirement will depend on the severity and risk of the vulnerability. Such tracking of vulnerabilities must be done through the company's change management tool and in accordance with the Change Management Process.

The information obtained from the vulnerability scanning process will be shared with appropriate personnel throughout the organization on a “need to know” basis to help eliminate similar vulnerabilities in other information systems.

Patching

All system components, software and production environments shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

System and Non-Company Application Patching

Patching includes updates to all operating systems and third party applications as provided by the appropriate vendor.

The AET Application Patching
The AET applications are patched in accordance with the Change Management Policy. Patches deemed to be of a high or critical nature may be rolled out in a compressed schedule as set forth in such policy.

Patching Exceptions
Patching production systems (e.g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigating alternative should be determined through a documented risk analysis.

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.