The AET

Access Control and Termination Policy

Purpose and Scope

This Access Control and Termination Policy defines requirements for access and removal of access to The AET data, systems, facilities, and networks. 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 or approved devices 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.

Access Control Requirements

Principle of Least Privilege

The AET adheres to the principle of least privilege, specifying that users of The AET systems will be given minimum access to data and systems based on job function, business requirements, or need-to-know for that specific user. Access to systems should be provisioned via a deny-all methodology - users should only gain access to a system upon receiving formal independent approval.

Administrative access to production servers and databases is restricted based on the principle of least privilege for personnel who have a job function and business need for such access.

Access to systems and applications must be controlled by a secure log-on process to prove the identity of the user.

Unique Accounts

Users of The AET systems and applications will be provided with unique credentials (IDs, keys, etc.) that can be used to trace activities to the individual responsible for that account. Shared user accounts shall only be utilized in circumstances where there is a clear business benefit and when user functions do not need to be traced. Shared account password should only be stored in a The AET approved password manager.

Password Security

Unique accounts and passwords are required for all users. Passwords must be kept confidential and not shared with multiple users. Where possible, all user and system account passwords must be a minimum of eight characters and complex. All accounts must use unique passwords not used elsewhere.

Rotation Requirements

If an account is suspected to be compromised, the password should be reset and the security team should be immediately notified.

Storing Passwords

Passwords must only be stored using a The AET approved password manager. The AET does not hard code passwords or embed credentials in static code.

Multi-Factor Authentication

When available, multi-factor authentication should be used. Multi-factor authentication must be used for access to company email, version control tool and cloud infrastructure.

Onboarding Procedures

In order to onboard new personnel, the following steps should be taken and documented:

1. Any The AET devices provided to the new hire must be inventoried in accordance with The AET policy
2. A new hire email or ticket must be sent to the appropriate team to inform them of new personnel
3. IT/Engineering and the new personnel's manager must document a checklist of accounts and permission levels needed for that hire
4. The applicable team must set up each user with the appropriate access, both logical and physical
5. All of the onboarding processes must be appropriately documented via ticketing or other document management tools

Offboarding Procedures

In order to offboard an employee or contractor, the following steps must be taken:

1. An offboarding email or ticket must be sent to IT/Engineering when personnel has been terminated or resigned informing IT/Engineering of the team members' last day
2. IT/Engineering must review and perform action against the appropriate revocation checklist to revoke access to The AET systems, applications, and physical access points (as applicable) within 24 hours of the last day with the company or sooner if necessary
3. Any The AET devices provided must be collected and accounted for in accordance with The AET policy
4. All of the offboarding processes must be appropriately documented via The AET ticketing or other document management tools

Changes to Access

Requests for changes to access level(s), such as in the cases of a change in job duties or an emergency requiring elevated permissions, must be documented and approved by the appropriate manager.

A documented request must be sent to the appropriate department when an employee or contractor role changes to evaluate whether access privileges should be changed. When accounts are no longer required, user access rights must be reviewed and reallocated as necessary prior to changes being made.

Such changes must be tracked using the The AET ticketing or other document management tools.

Quarterly Access Reviews

A team manager must review, audit, and document user accounts and associated privileges of at least high-risk and critical systems at least quarterly to ensure that access is restricted appropriately.

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.