The AET

Acceptable Use Policy

Purpose and Scope

This Acceptable Use Policy defines standards for appropriate and secure use of The AET's hardware and electronic systems including storage media, communication tools and internet access. 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 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.

General

Ownership

The AET is the owner of all company-issued hardware and electronic systems including the data stored in them or transmitted from them.

User Responsibilities

Personnel should not make any discriminatory, disparaging, defamatory or harassing comments when discussing The AET. Discussing The AET includes the use of social media, blogging or otherwise engaging in any conduct to the detriment of The AET.

Personal Use Systems

Personal use of The AET electronic systems is permitted provided such use does not interfere with productivity, confidentiality or the business and is not in conflict with team member responsibilities outlined in any The AET policy.

Compliance

- For security and network maintenance purposes, The AET may monitor and track system access and content of The AET hardware, system(s) and information to reasonably ensure compliance with applicable laws, regulations and The AET policies
- The AET reserves the right to access and audit any devices, networks and systems to ensure compliance with any The AET policy

Communication Tools

Use of Email and Messaging Tools

Email and other messaging tools are intended to be used as a business tools to facilitate communications and the exchange of information needed by team members to perform their assigned duties.

Encryption

All messages and/or attachments that contain confidential information are required to be encrypted to protect the privacy of the information.

Responsibilities

- Passwords should not be shared with another individual. They are intended for the authorized team member only
- Team members who transmit confidential information outside the organization should comply with applicable regulatory requirements, customer requirements, and The AET policies regarding the disclosure of confidential information to third parties
- Communications may be monitored and tracked without consent or advanced notice to the team member
- Retention and disposal of electronic communications should be in accordance with all The AET data protection and privacy policies

Prohibited Uses of Communication Tools

- Dissemination of confidential or protected information (i.e., trade secrets, team member personal information or financial data, customer information, etc.), except for approved business purposes
- Attempting to gain access to another team member’s account, without permission
- Misrepresenting, obscuring, suppressing, or replacing a team member’s identity
- Sending confidential information over an open network (the Internet) without proper encryption
- Transmitting, retrieving, or storing any communications or materials of a defamatory, discriminatory, harassing, or obscene nature
- Transmitting messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference

Devices

Use of Company Devices

The use of The AET phones (static and mobile), laptops and other hardware is primarily for business use.

Use of Personal Devices (BYOD)

The use of a personal device for The AET purposes should be limited to email and the The AET messaging tool unless there is business justification and formal approval. Personnel must not save The AET data to any personal device. Personnel are responsible for configuring their device to be in alignment with the device configuration settings specified in the next section of this policy.

Personal phones are not in scope for this policy.

Mobile Device Management (MDM)

Mobile device management (MDM) is implemented to manage and enforce mobile device configuration and security policies. Mobile devices must be approved prior to granting access to resources.

The MDM solution should ensure and/or manage the following:

- **Encryption:** User endpoint storage is encrypted at rest (e.g. FileVault for MacOS or Bitlocker for Windows)
- **Security Updates**: OS security updates are enforced and monitored
- **Malware Protection**: Malware protection is enabled (e.g XProtect for MacOS, Defender for Windows, or ClamAV for Linux)
- **Screensaver / Lockscreen**: Screensavers / lockscreens are configured to activate after a maximum of 15 minutes
- **Logging**: Logs are captured and stored to assist with security investigations
- **Password Policy**: Required passwords must align with The AET's Access Control and Termination Policy
- **Firewall**: Local firewall is enabled to provide layered host protection unless it interferes with development activities
- **Remote Wipe** (*Optional*):In the event of employee departure or theft, the mobile devices can be remotely wiped

Employees and applicable contractors must report loss, theft, or other security incidents related to their company-provided mobile device in a timely manner.

Use of Removable Media

The AET personnel must only use approved removable media on their work computers. Sensitive information must only be stored on removable media only when required in the performance of assigned duties and upon management's approval. When sensitive information is stored on removable media, it must be encrypted in accordance with the The AET Encryption and Key Management Policy. Exceptions to this requirement may be granted by senior management.

Responsibilities

- Personal use of The AET devices are allowed only as set forth in the General section of this policy
- Personnel assigned a The AET device are responsible for protecting the device from theft or damage
- If the issued device is lost or stolen, personnel responsible for the device must report the loss or theft to
- Devices that have not been approved by management should not be used to send or store any confidential information

Social Media

Limited and occasional use of The AET devices to access social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate The AET policies, is not detrimental to the best interests of The AET, and does not interfere with a team members regular work duties.

Networks and Internet Access

Responsibilities

- Use of internet access is primarily for business use. Personal use is allowed only as set forth in this policy
- Access to the The AET production network must be secure
- No confidential information shall be sent from to an individual or entity outside of The AET using personal email accounts
- Personnel must use the production network and internet only for lawful purposes

Encryption

The AET users who are in travel status and use laptops to access the production network or company data should reasonably ensure such transmissions are encrypted and only access the network through authorized means. During travel, access to the internet should only be made via secure wireless networks.

Explicit Content

Users using The AET devices who discover they have connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material must immediately leave the site and report such use to .

Prohibited Uses

You agree not to use personal email accounts for, but not limited to:

- Dissemination of confidential information
- Attempting to gain access to another Internet account, without permission
- Sending confidential information over the Internet without proper encryption

You agree not to use network and internet access to:

- Violate any applicable federal, state, local, or international law or regulation (including, without limitation, any laws regarding the export of data or software to and from the US or other countries).
- Access data, a server or an account for any purpose other than conducting The AET business, even if you have authorized access
- Make statements about warranty, expressly or implied, unless it is a part of normal job duties
- Make fraudulent offers of products, items, or services originating from any The AET account
- For the purpose of exploiting, harming, or attempting to exploit or harm, minors in any way by exposing them to inappropriate content, asking for personally identifiable information, or otherwise
- Send, knowingly receive, upload, download, use, or re-use any material which violates the rights of any individual or entity established in any jurisdiction
- Transmit, or procure the sending of, any advertising or promotional material, including any "junk mail," "chain letter," "spam," or any other similar solicitation
- Impersonate or attempt to impersonate The AET, an employee, contractor, another user, or any other person or entity (including, without limitation, by using e-mail addresses or screen names associated with any of the foregoing)
- Engage in any other conduct that restricts or inhibits anyone's use of the network, or which, as determined by us, may harm The AET or users of the network or expose them to liability
- Disable, overburden, damage, or impair the network or interfere with any other party's use of the network, including their ability to engage in real time activities through the network
- Use any robot, spider, or other automatic device, process, or means to access the network for any purpose, including monitoring or copying any network traffic or resources available on the network
- Use any manual process to monitor or copy any network traffic or resources available on the network or for any other unauthorized purpose without The AET's prior written consent
- Use any device, software, or routine that interferes with the proper working of the network
- Introduce any viruses, honeypots, trojan horses, worms, logic bombs, or other software or material which is malicious or technologically harmful
- Attempt to gain unauthorized access to, interfere with, damage, or disrupt any parts of the network or any server, computer, database, or other resource or element connected to the network
- Violate, attempt to violate, or knowingly facilitate the violation of the security or integrity of the network
- Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications

Content Standards

You agree not to send, knowingly receive, upload, download, use, or re-use any material which:

- Contains any material that is defamatory, obscene, indecent, abusive, offensive, harassing, violent, hateful, inflammatory, or otherwise objectionable.
- Promotes sexually explicit or pornographic material, violence, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.
- Infringes any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any other person.
- Violates the legal rights (including the rights of publicity and privacy) of others or contains any material that could give rise to any civil or criminal liability under applicable laws or regulations.
- Is likely to deceive any person.
- Promotes any illegal activity, or advocates, promotes, or assists any unlawful act.
- Causes annoyance, inconvenience, or needless anxiety or is likely to upset, embarrass, alarm any other person.
- Impersonates any person, or misrepresents your identity or affiliation with any person or organization.
- Gives the impression that material emanates from or is endorsed by The AET or any other person or entity, if this is not the case.

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.