The AET

Data Classification Policy

Purpose and Scope

This Data Classification Policy provides the basis for protecting the confidentiality of data at The AET by establishing a data classification system. 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 data 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.

Classification Management

All The AET data should be classified into one of the following four classifications:

1. Restricted Data,
2. Confidential Data,
3. Internal Data, and
4. Public Data.

All data that is not explicitly classified should be treated as confidential data and a classification should be determined and documented.

The examples below are not exhaustive. Data owners and senior management are responsible for assigning the types of ways certain data can be used as well as assigning the appropriate classification to The AET data.

If you are unable to determine the appropriate data owner or a classification for the data or believe certain data should be reclassified, please contact .

Changes to the classification of data must be approved by senior management.

Classification Levels

Public Data

Public data is information that may be disclosed to any person regardless of their affiliation with The AET. The Public classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that does not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside The AET and no steps need be taken to prevent its distribution. Public data can be retained for an indefinite period of time.

Examples of Public data include:

- published press releases;
- published documentation,
- published blog posts,
- anything on the The AET public website, and
- anything on The AET social media profiles

Internal Data

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data should be classified as such when the unauthorized disclosure, alteration, or destruction of that data would result in moderate risk to The AET, its customers, or its partners. Internal data generally should not be disclosed outside of The AET without the permission of the data owner. It is the responsibility of the data owner to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your manager or send an email to .

Examples of Internal data include:

- unpublished The AET memos,
- unpublished marketing materials,

- non-public The AET customer and partner names, and
- procedural documentation that should remain private

Confidential Data

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or The AET. This classification also includes data that The AET may be required to keep confidential, either by law or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Confidential data should be retained for only as long as it is needed to conduct internal/external business operations. Customer deletion requests and contractual deletion obligations should be the main source of authority for storing/deleting Confidential data.

Any unauthorized disclosure or loss of Confidential data must be reported to .

Examples of Confidential data include:

- individual employment information, including salary, benefits and performance evaluations for current, former, and prospective employees,
- legal documents,
- customer data,
- contractual agreements,
- compliance reports such as SOC 2,
- data that is subject to an NDA or other confidentiality clause, and
- information shared by partners or investors

Restricted Data

Restricted data includes any information that The AET has a legal or regulatory obligation to safeguard in the most stringent manner. Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to The AET, its customers, or its partners. The highest level of security controls should be applied to Restricted data.

Examples of Restricted data include:

- The AET codebase,
- intellectual property,
- passwords, private keys and other credentials,
- bank information,
- tax ids,
- information related to pending litigation or investigations,
- data required to be protected by regulatory obligations, and
- additional employment information such as background checks, health and medical information, social security numbers

Restricted data should be used only when no alternative exists and must be carefully protected. Regulatory data retention requirements should be the main source of authority for storing/deleting restricted data, as applicable, unless stricter organizational requirements have been enacted. Any unauthorized disclosure, unauthorized modification, or loss of Restricted data must be immediately reported to your manager and .

Data Handling and Labeling

All personnel accessing classified information must follow the rules listed above. Each incident related to handling classified information must be reported in accordance with the Security Incident Response Plan.

All types and forms (e.g. digital, physical) of data should be clearly labeled, denoting respective classification tiers. As mentioned above, all data not explicitly classified must be treated as if it were confidential data. Classification tiers with labels are listed below:

- Public Data -> "FOR PUBLIC USE"
- Internal Data -> "CLASSIFICATION: INTERNAL"
- Confidential Data -> "CLASSIFICATION: CONFIDENTIAL"
- Restricted Data -> "CLASSIFICATION: RESTRICTED"

All physical (e.g. paper, posters, etc.) and digital (e.g. Word/Google Docs, Excel/Google Sheets, PowerPoint/Google Slides) media should have a footnote clearly stating the proper classification level at the bottom of each page/sheet/slide.

Data Storage

Personnel should be mindful of where to store data based on the degree of classification. Where possible, personnel should observe the principle of least privilege, or sharing only what absolutely needs to be known. For example, there is no need to share restricted data to persons who do not have the need to know. Personnel should be especially mindful when sharing data to external users outside of the company.

Data Deletion

The method for secure erasure and destruction of media is prescribed in the Configuration and Asset Management Policy and Data Retention and Disposal Policy.

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

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.