Data Classification Policy

Version 2.6

Document version control page
Prepared By

Version	Date	Author	Update Description
1.0	12/06/08	JayaseelanJ	Initial Issue
1.1	22/08/08	JayaseelanJ	Format changes
1.2	10/09/09	JayaseelanJ	Policy Document Reviewed
1.3	12/07/2010	J.Jayaseelan	Policy Document Reviewed
1.4	25/11/2011	Jayaseelan J	Policy Document Reviewed and ISM Name changed to ISH
1.5	27/06/2012	Jayaseelan J	Policy Document Reviewed
1.6	27/06/2013	Jayaseelan J	Policy Document Reviewed
1.7	21/06/2014	Jayaseelan J	Policy Document Reviewed
1.8	01/08/2014	Jayaseelan J	Policy Document Reviewed as per ISO 27001:2013 requirement
1.9	22/06/2015	Jayaseelan J	Policy Document Reviewed
2.0	14/06/2016	Jayaseelan J	Policy Document Reviewed
2.1	15/11/2017	Santhosh S	Policy Document Reviewed
2.2	12/06/2018	Santhosh S	Policy Document Reviewed
2.3	10/07/2019	Santhosh S	Policy Document Reviewed
2.4	09/11/2020	Santhosh S	Policy Document Reviewed
2.5	06/12/2021	Santhosh S	Policy Document Reviewed
2.6	02/12/2022	Santhosh S	Policy Document Reviewed

Reviewed and Approved By

Version	Date	Reviewed by	Approved By	Owner
1.0	12/06/08	Mr. Madhavaswamy	Mr. R.Kumar	ISM
1.1	22/08/08	Mr. Madhavaswamy	Mr. R.Kumar	ISM
1.2	10/09/09	HR Director	Mr. R.Kumar	ISM

1.3	13/07/2010	HR Director	Mr. R.Kumar	ISM
1.4	28/11/2011	HR Director	Mr. R.Kumar	ISH
1.5	27/06/2012	HR Director	Mr. R.Kumar	ISH
1.6	28/06/2013	HR Director	Mr. R.Kumar	ISH
1.7	21/06/2014	HR Director	Mr. R.Kumar	ISH
1.8	01/08/2014	HR Director	Mr. R.Kumar	ISH
1.9	22/06/2015	HR Director	Mr. R.Kumar	ISH
2.0	14/06/2016	HR Director	Mr. R.Kumar	ISH
2.1	15/11/2017	HR Director	Mr. R.Kumar	ISH
2.2	12/06/2018	HR Director	Mr. R.Kumar	ISH
2.3	10/07/2019	HR Director	Mr. R.Kumar	ISH
2.4	09/11/2020	HR Director	Mr. R.Kumar	ISH
2.5	06/12/2021	HR Director	Mr. R.Kumar	ISH
2.6	02/12/2022	HR Director	Mr. R.Kumar	ISH

1. PURPOSE

The purpose of this policy is to provide all users of AEL Data to familiarize them of the Data Classification system being used in the Organisation.

2. SCOPE

This policy applies to all users who are using any kind of documented information's related to business activities of AEL Data.

3. ROLES AND RESPONSIBILITIES

All users using the AEL Data business activity related documented information's are responsible for adhering to this policy.

4. REFERENCE STATEMENTS

Information created, stored or processed by AEL Data shall be classified by Workers (if they created the information), or
Data Owners (for information systems or customer data) according to the following classification scheme:

- Public
- Internal
- Confidential
- Restricted

All Workers must consider information to be governed by the principle of "need-to-know." Unless a Worker has reason to access information in the performance of his or her defined job duties, access is denied.

Workers shall not disclose non-Public information to anyone who is not authorized to have it. This includes disclosure through oral and written means, whether electronic or otherwise.
Any questions as to whether information is Public, Internal or confidential, should be presented to the classifying Worker, or the applicable Data Owner, for determination. In the event the Worker or applicable Data Owner cannot be readily identified, direct all such questions to the ISS.

4.1. Public Information

Public information is information that is freely available to the general public, or whose release will not cause any harm to AEL Data. Examples of Public information include marketing literature, annual reports, and other materials specifically created by the marketing department for public release.
There are no special handling or disposal requirements for Public information and no special markings are required.

4.2. Internal Information

Internal is the default classification of data at AEL Data and includes all of AEL Data internal business correspondence, documented information's, and data created in the normal course of business which is not otherwise classified as confidential or Restricted. This includes all business email as well as all correspondences with clients.
All non-marked material, which is not Confidential Information, must be treated as Internal (i.e.,not released to outside parties or maintained on a need-to-know basis) until it is confirmed as Public information.
There are no special markings required for printed or electronic internal information. Printed internal information must be destroyed using the shredded.

4.3. Confidential Information

Confidential information includes all of AEL Data business, financial and technical information including, without limitation, customer, product, pricing and product development plans, network and system diagrams or other non-restricted information, documented information's or data create in the normal course of business which if made public would cause harm to AEL Data.
Confidential information also includes information which is obtained by AEL Data or to which AEL Data otherwise had access to, under obligations of confidentiality to a third party, whether under a confidentiality agreement, non-disclosure agreement, or other agreement.
If information is Confidential, it must be marked "AEL Data Confidential" before being distributed or exposed to a non- AEL Data party, regardless of distribution method (e.g., written form, email, via facsimile, etc.) and then only under a AEL Data approved non-disclosure or similar agreement.
Confidential information concerning AEL Data networks or systems must be approved for release by the ISC prior to distribution to non- AEL Data 3rd parties.
Confidential information must be destroyed using the secure document disposal facilities provided at AEL Data business locations, or, if on paper, DVD or CD media it can be cross shredded.
Confidential information contained or stored in other media must be disposed of in accordance with the instructions of the ISC.

4.4. Restricted Information

Restricted information includes all of the AEL Data important business documented information's which could harm AEL Data in terms of hampering various business activities like important

financial transactions; deals with other Organisation which if made public could harm the entire Organisation.

- Restricted information should not be collected and stored unless absolutely necessary.
- Access to restricted information should be authorized only as needed to perform assigned duties.
- Delete restricted data when there is no longer a business need for its retention.
- Avoid using actual data when testing an application; rather "mask" the restricted data, such as the Social Security Number, with dummy information. If this is not possible, ensure implementation of appropriate security measures.
- When restricted information is distributed, include notification that the data is restricted and that it requires specific security protection.
- Restricted data should not be stored on portable devices. If it is necessary to store restricted data on portable devices, ensure the appropriate protections measures, such as encryption, are in place before installing restricted data on the device.

5. COMPLAINCE

5.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.
5.2. Audits will be managed in accordance with the Information Security Audit Procedure.
5.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

6. EXCLUSION

There are no exclusions to the above guidelines

7. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action as per HR & Admin Procedure.