Clear Desk 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	27/06/2013	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	02/12/2023	HR Director	Mr. R. Kumar	ISH

1. PURPOSE

Information is an asset which, like other important business assets, has value to AEL Data and consequently needs to be suitable protected.
Information, in whatever form it takes, or means by which it is shared or stored, should always be appropriately protected. Information security is characterised as the preservation of:
• Confidentiality: ensuring that information is accessible only to these authorised to have access;
• Integrity: safeguarding the accuracy and completeness of information and processing methods;
• Availability: ensuring that authorised users have access to information when required.

Confidentiality, integrity and availability of information is very essential to maintain legal compliance.

2. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at AEL Data, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by AEL Data.

3. ROLES AND RESPONSIBILITIES

All users of AEL Data having any Information asset of the Organisation must adhere to this policy.

4. REFERENCE STATEMENT

To improve the security and confidentiality of information, wherever possible all users of AEL Data should adopt a clear desk policy for papers.

This can be ensured by following the below given guidelines:

- Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards etc are not available, office / room doors must be locked if left unattended. At the end of each session all sensitive information should be removed from the work place and stored in a locked area. This includes all employee identifiable information, as well as business critical information such as salaries and contracts.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- It is good practice to lock all the rooms specifically of the CEO and CISO when they are not in use.
- Any visit, appointment or message books should be stored in a locked area when not in use.
- The reception desk can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times in particular for employees and third party visitors identifiable information should not be held on the desk within reach/sight of visitors.
- It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

5. COMPLIANCE

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.