Clear Screen Policy

Version 2.7

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
2.7	05/12/2023	`Muthukrishnan B	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
2.7	05/12/2023	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 are 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 STATEMENTS

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:

- AEL Data computers / computer terminals should not be left logged on when unattended and should be password protected.

- Computer screens should be angled away from the view of unauthorised persons.
- The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period of time.
- The Windows Security Lock should be password protected for reactivation.
- Users should log off their machines when they leave the room.
- Where possible other security devices, such as keypads, should be introduced to areas that are only accessible to staff.

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.