Mobile Computing Security 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 have a clear understanding of proper procedure and usage.

2. SCOPE

This policy applies to all employees and vendors of AEL Data

3. ROLES AND RESPONSIBILITIES

- **IT department** is responsible of maintaining all documented information's of mobile devices being used in AEL Data.
- **Admin / Security department** is to ensure proper checking of mobile devices by the security guards as laid down in the Policy.
- **User** is responsible for the security and proper usage of Mobile devices.

4. REFERENCE STATEMENTS

4.1. Mobile devices are not to be carried on the production floor.
4.2. Official emails and documented information's are only to be used on the mobile device if the mobile device supports the following security features:
- Emails must to be encrypted when in transit.
- The mobile device must be password protected, refer the password policy for help selecting a strong password.
- All emails and documented information's needs to be encrypted with minimum 256bit encryption when stored on the mobile device.

4.3. IT support must be informed in case the device is stolen or missing immediately.

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. EXCLUSIONS

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.