Laptop 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

In today's mobile computing environment, it is not unusual to keep sensitive data on laptops. Protecting laptop data confidentiality requires a layered approach at both physical and logical access levels. Necessary security measures should be taken to ensure data security of data residing in the Laptop and also proper accountability and distribution/issue of Laptops. To frame a laptop security policy to:

- Ensure adequate mode of computing when away from office for Organization business purposes.
- Minimize the security risk and information leakage.

2. SCOPE

All laptops being taken in and out of Company premises and used by the users and IT Department.

3. ROLES AND RESPONSIBILITIES

- **IT department** is responsible of maintaining all documented information's of Laptop inventory, Issue, returning and repair as laid down in the policy.
- **Admin/ Security department** is to ensure proper checking of Laptop by the security guards as laid down in the Policy.
- **User** is responsible for the security and proper usage of Laptops.

4. REFERENCE STATEMENTS

4.1. Laptops should be used strictly for Company business purposes only.
4.2. BIOS must be password protected.
4.3. BIOS Boot password, i.e. power-on password must be set
4.4. Each laptop should be engraved / pasted an asset tag.
4.5. All laptops should be insured against fire, theft, mechanical and electrical damages.
4.6. Backup of critical data of laptop should to be taken at regular intervals and especially before taking to outstation.
4.7. The security of the laptop is the responsibility of the person carrying it.
4.8. Employees should keep their laptops in the office, inside locked cabinets or Kingston cable lock before leaving from the office.
4.9. Laptops should not be left unattended at public places.
4.10 In order to save inconveniences, a notice should be displayed at the entry gates and a copy be given to the security guards, requesting visitors to show their laptops for verification.
4.11Laptops must have power on password in BIOS for protection from unauthorized use.
4.12 A record of all Laptops must be maintained in accordance with Asset Management Policy.
4.13 Employees who are issued the laptop ensure that all the data is erased before returning the laptop.
4.14 Security guards must check all visitor laptops being taken in and out of Organization site and note down Make and serial numbers of the Laptops.

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.