Physical 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

AEL Data physical security foundation would help the Organisation to protect and preserves information, physical assets, and human assets by reducing the exposure to various physical threats that can produce a disruption or denial of computer service.

2. SCOPE

This policy applies to all users entering the AEL Data premises.

3. ROLES AND RESPONSIBILITIES

Manager Admin, IT & IS Head and all users within AEL Data are responsible for ensuring the Physical security of the Organisation.

4. REFERENCE STATEMENTS

In order to ensure that AEL Data facilities are properly secured, security controls shall be implemented for all facilities. Access Controls - Shall include a minimum of locked doors to access the facility, except in those facilities where a receptionist is available to provide a buffer for access to the work spaces.
In addition to the access controls defined, facilities are required to meet AEL Data server room standards for a development environment, including but not limited to the following:

- Power and Environmental controls and appropriate power redundancy or backup
- Cabling access, routing and security
- Practical elimination of identified single points of failure
- Regular and preventative maintenance
- Twenty-four hour environmental monitoring controls
- Isolation of data center areas from delivery and loading areas

4.1. Employee & Vendor Access

The facility manager is responsible for documenting and following an on-going process to ensure that Vendor access to facilities is provided as necessary to perform their job duties. This process should be audited on a periodic basis by the ISC to ensure that terminated Employee have been removed and to ensure that Employee have been granted access only to those areas necessary to do their jobs.
Vendors are responsible for safeguarding their Visitor Pass Biometric Access. Lost Visitor Pass or Biometric Access shall be reported to the Facilities department immediately. Vendors shall not allow unauthorized personnel to follow them into secured area (no tailgating), and should not prop open or hold open controlled-area or exterior doors.
Employees shall not enter secured rooms that they have not been granted access to, unless accompanied by an authorized Worker and unless they have a proper need to enter the secured rooms.
Access to all facilities shall be immediately terminated upon Employees resignation or dismissal and all access cards, badges or devices shall be retrieved from the Worker.

4.2. Photo Identification Card

At those AEL Data facilities that provide photo identification badges,. Workers shall wear their badges at all times while on AEL Data property. ID Cards should be worn on a person's front side at or above the waistline.
Employees who have lost or had their photo ID Card stolen must immediately report the incident to the Facilities department. Workers who have a damaged photo ID Card shall request a replacement card. Any Employee needing a new ID Card to reflect a change in name shall request an updated Card. Any employee with a significant change in facial appearance, such as the

growing or removal of a beard or mustache, or adding or removing glasses shall request an updated Card.
Temporary ID Card should be worn in place of the photo ID Card until a replacement photo ID badge is Card.
Employee encountering a person not wearing a badge and not recognizing him or her as being a Employee shall take one of the following actions:
1. Ask for the name of the Employee they are visiting and escort them to that person after calling to confirm
2. Escort them to where they can be issued an appropriate badge
3. Contact the security guard, Facilities Manager, site security representative to have them removed from the building. Employee must not physically try to remove or restrain the person while doing so.
4. Only five Temporary access cards would be made available as an alternate.
5. Each Associate can request for temporary access cards only once in a month
6. Associates violating policy would be informed to Senior Management, Linkage to Performance appraisal
7. Monthly Violation would be published by Facilities & Administration.

4.3. Visitors

All visitors to AEL Data facilities must enter through the location's main lobby, sign in and out of visitor log books and must wear visitor Pass at all times while on AEL Data premises.
Visitors must be escorted by a AEL Data employee while inside AEL Data data centre. Vendors using visitor Pass or temporary access cards must be accompanied by a AEL Data escort at all times.

4.4. Workspace Security

Employees are responsible for the security of their workspace. AEL Data provides locked storage at all facilities for personal valuables and company property. AEL Data is not responsible for loss of Employees personal property. Workers are responsible for securing their laptop computers when away from the office. If laptops are left overnight in a AEL Data office they must either be locked using a locking cable, stored in a locked drawer or cabinet or the office must be locked. Automatic screen savers must be used on all workstations and laptops to ensure that the screen and/or workstation are locked whenever the equipment is left unattended for 10 minutes or more. Employees shall lock their workstation screens manually whenever they leave them rather than wait for the automatic screen saver to engage. Employee shall also logoff their workstations at the end of the day rather than locking them, unless it is required to leave a workstation logged on due to a special process or job which is running.
Employees should ensure that Confidential Information in their area such as papers, reports, printouts, data media, whiteboard drawings are secured when left unattended.

4.5. Removal of Property

Fixed asset computer and network equipment, with the exception of laptops, may not be removed from AEL Data offices without prior approval from authorized AEL Data management. When necessary and appropriate, equipment should be logged out. It is the responsibility of the Facilities Department to enforce authorization and control procedures that ensure AEL Data assets are removed from AEL Data facilities for business purposes only.

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. 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.