Access Control 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

Access Control Policy is define in order to minimise the exposure of AEL Data from destruction, theft and loss (eg. Confidentiality and Integrity), disruption to business operations and a damage to AEL Data brand image which may follow from unauthorised use of its electronic resources.

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 using the AEL Data network and resources must adhere to this policy.

4. RELATED Documented Information's

Information Security Audit Procedure
Password Policy
Acceptable Encryption Use policy

5. REFERENCE STATEMENTS

Access control policies provide details on controlling access to information and systems, with these topics typically covered at some length including the management of a number of key issues such as User ID's, Password, Remote Access, Remote access Software and Hardware which are covered in details as given below.

5.1. User IDs

These are the types of IDs in use at AEL Data:

- User Account IDs - accounts for general users, customers, and those persons accessing computers, applications, databases and systems in a non administrative function.

- Process IDs - accounts for applications, databases, and other automated processes.
- Privileged Account IDs - accounts for administration of servers, network devices, Biometric Device, etc.

All access control systems (network, domains, servers, applications, database management systems, workstations) shall utilize unique, individual User Account IDs for each employee. Any default user ID that was installed with any application, operating system or device shall have the password changed upon installation or removal, as appropriate.
Privileged Account IDs and Process IDs are issued for use and management of applications, devices and systems. Privileged Account IDs and Process IDs cannot be used by individuals for personal use nor can they be used outside of the application.
Passwords for these IDs must be closely guarded and restricted to an as-needed basis only for the management of that application or system.

5.2. Password Management

Refer “Password Policy”

5.3. Remote Access

Remote access to AEL Data networks and systems from the Internet is permitted only through\ perimeter gateways specifically authorized by the ISC. The appropriate AEL Data IT group must log all connection.

5.4. Remote Access Software and Hardware

The use of any type of remote control software or hardware that enables a user to control or access data on a AEL Data system without utilizing an authorized perimeter gateways is prohibited without the prior written authorization of the ISC

6. COMPLIANCE

6.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.
6.2. Audits will be managed in accordance with the Information Security Audit Procedure.
6.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

7. EXCLUSION

There are no exclusions to the above guidelines.

8. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action as per HR & Admin Procedure.