Network Access Policy

Version 2.8

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
2.8	04/12/2024	Muthukrishnan B	Policy Document Reviwed

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
2.8	04/12/2024	HR Director	Mr.R.Kumar	ISH

1. PURPOSE

AEL Data network infrastructure is provided as a central utility for all users of AEL Data Information Resources. It is important that the infrastructure, which includes wireless and cabling and the associated ‘active equipment’, continues to develop with sufficient flexibility to meet AEL Data demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

2. SCOPE

The scope of Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of AEL Data information.

3. ROLES AND RESPONSIBILITIES

The responsibility of effective implementation of guidelines for Network Access policy applies to all individuals that are responsible for the use of Information Resources.

4. REFERENCE STATEMENTS

4.1. Network IP address will only be assigned by the IT team No user should change their IP address.

4.2. All remote access (dial in services) to AEL Data must be controlled with adequate security in place.

4.3. Remote users may connect to AEL Data Information Resources only through an approved modem and using protocols approved by AEL Data.

4.4. Users inside AEL Data firewall may not be connected to AEL Data network while at the same time a modem is being used to connect to an external network.

4.5. Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, firewall or wireless access point to AEL Data network without IT & IS Head‘s approval.

4.6. Users must not install network hardware or software that provides network services without AEL Data IT & IS Head’s approval.

4.7. Non AEL Data computer systems that require network connectivity must confirm to AEL Data IS Standards.

4.8. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, AEL Data users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to AEL Data network infrastructure.

4.9. Users are not permitted to alter network hardware in any way.

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.