End User Computing 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 set forth acceptable use of the AEL Data End-User Computing (EUC) computer equipment, software, and network facilities, to foster and maintain an environment where users have confidence in the integrity and security of those facilities, to ensure all applicable hardware inventory and software licensing requirements are met and to establish consistency in computer use procedures and regulations across AEL Data.

2. SCOPE

The scope of this policy includes networking, software and Information related to AEL Data business activities.

3. RESPONSIBILITIES

All employees, contractors and third party vendors are responsible for adhering to this policy.

4. REFERENCE STATEMENTS

4.1. Users' Responsibilities

General

- Users must comply with Acceptable Use Policy of AEL Data.

- Users must comply with Network Security Policy of AEL Data.
- Users are responsible for knowing and obeying the specific policies established for the system and networks they access.
- Users are responsible for respecting the rights of other users, including their rights as set forth in other policies; these rights include but are not limited to privacy, freedom from harassment, and freedom of expression.
- Users should respect the computing needs of others by not deliberately performing acts that are wasteful of computing resources or that unfairly utilise the resources.
- Information contained in computer files is to be accessed or used for authorized business purposes only. Casual browsing through computer files for personal reasons is strictly prohibited.
- Personal software may not be loaded on AEL Data Systems. Systems must not be used for commercial purposes nor should personal use interfere with normal business operations.
- Users shall not damage, alter or disrupt computer systems.

Security

To protect the information that resides in the AEL Data enterprise network a number of security measures have been implemented.

- Users are to have valid, authorized accounts and may only use those computing resources that are specifically authorized.
- Users are required to take reasonable steps to ensure the security of their account or facility. As a result, users should safeguard their accounts and not give anyone else access to their accounts or other user accounts. Users' authorization to use a facility is not transferable to others.
- Users may not try in any way to obtain a password for another user's account.
- Data protection schemes and system security exists to protect all users. Users must not attempt to circumvent data protection schemes or exploit security loopholes.
- Users may only modify software, which is intended to be user customized. No other software modifications are allowed without the approval of the IT dept.
- To ensure additional security, users must:
    - Protect their password from disclosure to others.
    - Choose passwords that are not obvious. A good password includes a combination of letters, numbers and symbols.
    - Not write their passwords down.
- Users shall disclose to the AEL Data IT Team of the misuses of computing resources or potential loopholes in computer systems security and cooperate with the IT Team in the investigation of system abuses.

Fraudulent Use or Behavior

- Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

- Network security is a very serious issue. Tampering with data or attempting to circumvent the flow of data is strictly prohibited. Disciplinary action will occur whenever a breach of security or hacking is detected and determined intentional.

- Correct identification of network data and network users is essential to shared network operations. Users may not misrepresent themselves or their data on the network.

- Users must not use the AEL Data network resources to gain or attempt to gain unauthorized access to remote computers.

Software

No AEL Data employee or contractor shall engage in any activity that violates local laws with respect to intellectual property rights; the terms of software license agreements; or other AEL Data policies pertaining to computer software. With regards to copyright:

- Software used on AEL Data personal computers must be purchased and/or licensed issued for AEL Data.

- Users must not make software available for others to use or copy in violation of that software's license agreement.

- Unlicensed software from any third party should not be accepted.

- Illegal copies of computer software or unlicensed software may not be installed onto any AEL Data owned or operated computer system.

- No programs that could result in the eventual damage to a file or computer system and/or reproduction of itself may be loaded on AEL Data computers. This is directed toward, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.

Games

All computer systems are the property of AEL Data and are furnished to users for business use only. Entertainment through the use of computer games is not permitted.

Viruses

The threat of a virus infection can arise from downloading files from the Internet, loading data into your computer from a diskette, or running an e-mail attachment. All personal computer systems are loaded with anti-virus software. Users may not disable anti-virus software on the systems provided for their use.

Hardware

- All personal computer systems used by AEL Data employees are owned by AEL Data and managed by IT Dept. Employees and contractors using this equipment should not consider this equipment their personal computer equipment and are responsible for following policies and procedures developed by the IT Dept for the use of these facilities.

- Hardware inventories and network operations require an accurate count and accurate location guide of AEL Data computers. Personal computer equipment should not be relocated nor should the physical configuration or any AEL Data personal computer be modified without consultation with AEL Data IT Dept.

5. EXCEPTIONS

There are no exceptions to the above guidelines. Unless required for a specific application / purpose, this must be approved by CISO in writing.

6. ENFORCEMENT

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