Acceptable Use 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 and 5.2.9 statement added
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	05/12/202	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

Acceptable Use policy states outline the acceptable use of computer / IT equipment at AEL Data. These rules are in place to protect the employee data and AEL Data. Inappropriate use exposes AEL Data to risks including virus attacks, compromise of network systems and services, and legal issues.

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 AEL Data.

1. ROLES AND RESPONSIBILITIES

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

3. RELATED Documented Information’s

Email Usage Policy
Information Security Audit Procedure
Password Policy
Acceptable Encryption Use policy
Laptop Policy

4. REFERENCE STATEMENTS

4.1. General Use and Ownership

4.1.1. While AEL Data network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Organisation systems remains the property of AEL Data. Because of the need to protect AEL network, management cannot guarantee the confidentiality of information stored on any network device belonging to AEL Data.

4.1.2. For internet usage guidelines refer to the Internet Usage Policy.

4.1.3. For email usage guidelines refer to the Email Usage Policy.

4.1.4. It is recommended that any information that users consider sensitive or vulnerable be encrypted.

4.1.5. For security and network maintenance purposes, authorized individuals within AEL Data may monitor equipment, systems and network traffic at any time,

4.1.6. AEL Data reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

4.2.1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by Information classification guidelines. Examples of confidential information include but are not limited to: company private, Organisation strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

4.2.2. Users should manage their account passwords according to the password policy.

4.2.3. Users should lock or logoff their desktop when they leave their workstation.

4.2.4. Use encryption of information in compliance with Acceptable Encryption Use policy.

4.2.5. Since information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the Laptop Policy.

4.2.6. Postings by employees from a AEL Data email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of AEL Data, unless posting is in the course of business duties.

4.2.7. All hosts (workstations, Blackberry, mobile phones, network devices) used by the employee that are connected to the AEL Data Internet/Intranet/Extranet, whether owned by the employee or AEL Data, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

4.2.8. USB Hard Drive and USB Stick are used for the Scanner System, IT/IS Dept, and Management Peoples in AEL Data with Anti-Virus Scanning.

4.2.9. USB ports are enabled in the desktops for required projects (mobile devices/Tablets etc.,)

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of AEL Data authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing AEL Data -owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1.System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AEL Data.

4.3.1.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AEL Data or the end user does not have an active license is strictly prohibited.

4.3.1.3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.3.1.5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.6. Using a AEL Data computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.3.1.7. Making fraudulent offers of products, items, or services originating from any AEL Data account.

4.3.1.8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.3.1.9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.3.1.10. Port scanning or security scanning is expressly prohibited unless prior notification to CISO is made.

4.3.1.11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.3.1.12. Circumventing user authentication or security of any host, network or account

4.3.1.13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.3.1.14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.15. Providing information about, or lists of, AEL Data employees to parties outside AEL Data.

4.3.2. Email and Communications Activities

4.3.2.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4.3.2.3. Unauthorized use, or forging, of email header information.

4.3.2.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.2.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6. Use of unsolicited email originating from within AEL Data networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by AEL Data or connected via AEL Data network.

4.3.2.7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

1. COMPLIANCE

1.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.

1.2. Audits will be managed in accordance with the Information Security Audit Procedure.

1.3. Every effort will be made to prevent audits from causing operational failures or disruptions.

2. EXCLUSION

There are no exclusions to the above guidelines

3. ENFORCEMENT

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