# *Email Usage 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

The purpose of this policy is to provide mail usage guidelines for the users of the AEL Data E-Mail service.

## 2. SCOPE

This policy applies to all users who use e-mail services provided by the AEL Data.

## 3. ROLES AND RESPONSIBILITIES

All users using the AEL Data e-mail services are responsible for adhering to this policy. An account found in violation of this policy may be suspended or terminated, depending on the severity of the abuse.

## 4. RELATED Documented information's

Password Policy
Encryption Policy

## 5. REFERENCE STATEMENTS

**5.1.** All users of AEL Data mail services are expected to conduct themselves in a professional and ethical manner.
**5.2.** All mails which transit through AEL Data network are stored in plain text /HTML/Rich test files. Users should note that no secrecy can be attributed to the mails in transit.
**5.3.** All mail users shall adhere to the Password Policy. Users shall keep their user-ids and passwords secure. They shall not reveal to others or allow others to use their user-ids or passwords.
**5.4.** Users are responsible for their accounts and may be held accountable if someone uses their accounts with permission and violates the policy.
**5.5.** Users shall not attempt any unauthorized access of intranet, Internet or mail services. Unauthorized access includes, for example, the distribution of messages anonymously, use of other officers' user-ids or using a false identity.
**5.6.** The AEL Data mail services shall be used in accordance with the law of the land, and may not be used as a vehicle to harass or intimidate anyone.
**5.7.** AEL Data reserves the right, without notice, to temporarily limit or restrict any individual's access to his email. This is intended to protect the integrity of AEL Data facilities and its use against unauthorized or improper use.
**5.8.** Users must use only those resources that AEL Data has authorized for their individual use. Users are authorized to access, use, copy, modify, or delete files and data on their own email account. Users are not authorized to perform any of these functions on another user's email account or a AEL Data system.
**5.9.** User privacy is not to be violated. It is the responsibility of the user to protect their privacy. Users should not leave confidential information on a screen where it could be viewed by an unauthorized person.
**5.10.** Users may not intentionally obscure, change, or forge the date, time, physical source, logical source, or other label or header information on electronic mail, files or reports.
**5.11.** All incoming and outgoing email will be scanned by antivirus software.

### 5.12. Virus Handling

5.12.1. Industry standard spam and gateway antivirus protection must be used.
5.12.2. Efforts are made to block virus and other harmful code coming to users' mailbox. Still there are chances that user may get mails with the latest virus infections.
5.12.3. Users shall take necessary actions as and when advised by the System administrator and/or IT & IS Head regarding virus handling.

5.12.4. IT Dept shall update client software packages to the latest versions and apply necessary patches as and when available with software vendors.

**5.12.5.** IT Dept must run anti virus software on their desktops and check for virus for all incoming/outgoing attachments.

## 6. COMPLAINCE

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. EXCLUSIONS

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.