Antivirus 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	27/06/2014	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	12/06/2019	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

To protect software & data by using of appropriate software, guidelines and security measures from

- Viruses
- Worms
- Trojans
- Other malicious code

2. SCOPE

This policy applies to all computers that are based within the Organisation network or are utilizing its resources through file directory sharing. The name of Computer includes:

- Desktops
- Laptops
- File/Web/FTP/Print Servers
- And other computer based equipments

3. ROLES AND RESPONSIBILITY

IT Services Desk

- They are responsible for creating procedures that ensure anti-virus software is running at regular intervals, and computers are verified as virus-free. Failure to do so would result in the compromise of the entire Organisation network and the valuable data that resides in it.

- They should also conduct sampling tests on employees' workstations to ensure that the latest virus signatures have been updated.

- A monthly report should be sent to the CISO giving the sample test report.

Users - The users must be familiar with the policy and follow the guidelines as stated in the policy.

4. REFERENCE STATEMENTS

4.1. All computers within AEL Data must have Management approved anti-virus (Third party & inbuilt) software installed.

4.2. Weekly scheduled scanning must be enabled to run at regular intervals.
4.3. Anti-virus software and the virus signature files must be kept up-to-date.
4.4. Virus-infected computers must be removed from the network until they are verified as virus-free.
4.5. Any activities with the intention to create and/or distribute malicious programs into AEL Data networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
4.6. Any occurrence of virus/worm like activity should be reported immediately to the IT Services Support Desk.
4.7. Computer files received from unknown source should not be opened till antivirus scanning has been done.
4.8. Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
4.9. Delete spam, chain, and other junk email without forwarding, as they may contain viruses.
4.10. Back-up critical data and system configurations on a regular basis and store the data in a safe place to safeguard from data loss due to virus attacks.
4.11. If operation conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the desired operation. After the operation, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
4.12. Antivirus report needs be generated on a 3 months once and shared with the CISO.

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. EXCEPTIONS

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

7. ENFORCEMENT

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