System Usage Monitoring 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	27/06/2014	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

INTRODUCTION

System Usage Monitoring Policy is a method used to confirm that the security practices and controls in place are being adhered to and are effectively being monitored and reviewed at periodic intervals.

1. PURPOSE

The objective of the System Usage Monitoring Policy is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed.

One of the benefits of System Usage Monitoring Policy is the early identification of wrong doing or new security vulnerabilities. This early identification can help to block the wrong doing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

2. ROLES AND RESPONSIBILITIES

The responsibility of effective implementation of guidelines for System Usage Monitoring Policy applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security.

3. REFERENCE STATEMENTS

3.1. Information Security tools will provide real time notification of detected malicious activity and vulnerability exploitation. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Traffic pattern on LAN and protocol wise distribution
- Operating system security parameters

3.2. The following files will be checked for signs of malicious activity and vulnerability exploitation at a frequency determined by risk:

- Intrusion Prevention System logs
- Firewall logs
- User account security logs
- Network scanning logs
- Data backup recovery logs
- IT trouble tickets related to IT Security incidents
- Network printer and fax logs

3.3. Any security issues discovered will be reported to the Chief Information Security Officer (CISO) for follow-up investigation.

4. COMPLIANCE

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

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

4.3. Every Effort will be made to prevent audits from causing operational failure or disruptions.

5. EXCLUSIONS

There are no exclusions to the above guidelines

6. ENFORCEMENT

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