Information Security 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	Muhukrishnan 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	CISO
1.1	22/08/08	Mr. Madhavaswamy	Mr. R.Kumar	CISO
1.2	10/09/09	HR Director	Mr. R.Kumar	CISO

1.3	13/07/2010	HR Director	Mr. R.Kumar	CISO
1.4	28/11/2011	HR Director	Mr. R.Kumar	CISO
1.5	27/06/2012	HR Director	Mr. R.Kumar	CISO
1.6	28/06/2013	HR Director	Mr. R.Kumar	CISO
1.7	21/06/2014	HR Director	Mr. R.Kumar	CISO
1.8	01/08/2014	HR Director	Mr. R.Kumar	CISO
1.9	22/06/2015	HR Director	Mr. R.Kumar	CISO
2.0	14/06/2016	HR Director	Mr. R. Kumar	CISO
2.1	15/11/2017	HR Director	Mr. R. Kumar	CISO
2.2	12/06/2018	HR Director	Mr. R. Kumar	CISO
2.3	10/07/2019	HR Director	Mr. R. Kumar	CISO
2.4	09/11/2020	HR Director	Mr. R. Kumar	CISO
2.5	06/12/2021	HR Director	Mr. R. Kumar	CISO
2.6	02/12/2022	HR Director	Mr. R. Kumar	CISO
2.7	05/12/2023	HR Director	Mr. R. Kumar	CISO

1. PURPOSE

Information Security policy states AEL Data is in the business of conversion and management of data and recognizes the vital importance of information security and is fully committed to protect the privacy and security of customer data. AEL has established an information security management system (ISMS) that covers all the processes required to protect information.

Information security: confidentiality, integrity and availability.

Confidentiality: Ensuring that information is accessible only to those authorized to have access

Integrity: Safeguarding the originality, accuracy and completeness of information and Information processing methods

Availability: Ensuring that authorized users have access to information as and when required

2. SCOPE

AEL Data is committed to protecting the customer's information. To achieve this goal, the company has implemented an Information Security Management System in accordance with ISO/IEC 27001:2013 and BIP 0008:Code of Practice on Legal Admissibility and Evidential Weight of Information Stored Electronically

Owner:

CISO is the owner of the Information security policy.

3. ROLES AND RESPONSIBILITIES

The Information Security Head (ISH) is responsible for maintaining the policy.

CISO

- Focus on business; security must support business initiatives and be an enabler for the business.
- Focus on risk management, not security for the sake of security; develop data classification and information risk management processes to direct resources towards the protection of high-risk, critical assets.
- Educate the senior executives, Business Managers, and the security staff on the link between good security and good business.
- Create a strong, effective security-awareness program for all employees, contractors and third party vendors and link company/personal success to good security and management of risk; enforce policies when bad behavior occurs.
- Hire and retain high quality staff which could act as ensuring effective security in the Organization.
- Fund the security program appropriately wherever required to reduce the risk to an acceptable level.
- Develop metrics; use a scorecard to measure continuous improvements and make sure the metrics are aligned with business objectives.

IT & IS Head

- Overall monitoring to detect breaches of security related policies.
- Manages the response to any computer security incidents.
- Maintains professional relationships with international security bodies or other professional forums.
- Carries out research in the areas of technical defenses and tools.
- Develops or customizes the security solutions for the Organization.
- Monitors online resources and issues appropriate security advisories to the employees.
- Liaises closely with the ISC regarding policy development and compliance.

IT Security Administrator

- Prepare and maintain security procedures that are or to be implemented in AEL Data according to the information security policies.
- Take reasonable precautions to guard against corruption, compromise or destruction of IT, e.g. conduct security scans of systems for which they are responsible, and conduct audits of passwords.
- Ensure the files of users remain private and secured from unauthorized access.
- Take reasonable and appropriate steps to see all hardware and software license agreements are faithfully executed.
- Limit access to administrative (privileged) accounts
- Notify all system security issues to the IT & IS Head.

Security Coordinators

- Accessing the risk to systems and developing plans to minimizing the potential threats
- Contingency planning for disaster recovery in the even of a disaster
- Making sure the procedure meet AEL Data information security policy
- Investigating actual breaches and carryout corrective actions

4. RELATED Documented Information's

Access Control Policy
Acceptable Use Policy
Analog ISDN Policy
Antivirus Policy
Backup Policy
Biometric Management Policy
Clear Desk Policy
Clear Screen Policy
CCTV Management Policy
Data Classification Policy
Data Retention Policy
Email Usage Policy
Encryption Policy

End user Computing Policy
Environmental Security Policy
Laptop Security Policy
Media Disposal Policy
Mobile Computing Security Policy
Network Access policy
Password Policy
Physical Security Policy
Privacy Policy
Risk Assessment Policy
Software Licensing Policy
Special Access Policy
System Usage Monitoring Policy
Sexual Harassment Policy
Third Party Access Policy
User Account management Policy
VAPT Policy
Web & FTP Server Security Policy
WorkStation Policy

5. Objectives

Information is only accessible to authorized persons from within or outside the company.
Confidentiality of information is maintained throughout its lifecycle.
Integrity of information is maintained throughout the various processes.
Information security Risks are identified and investigated.
Contractual Security obligations are assessed and conformed
Legal and statutory IS requirements are assessed and conformed.
Business continuity plans are established, maintained, and tested.
All personnel are trained on information security
Business requirements for availability of information and systems will be met.

This policy has been approved by the company management and shall be reviewed by the management review team Every Quarter.

6. COMPLIANCE

Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.
Every effort will be made to actions to address the risk and opportunities to prevent audits from causing operational failures or disruptions.

7. EXCLUSION

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.