Information Security Policy for supplier

Version 1.8

Document version control page

Prepared By

Version	Date	Author	Update Description
1.0	01/08/2014	JayaseelanJ	Initial Issue
1.1	22/06/2015	Jayaseelan J	Policy Document Reviewed & Updated
1.2	14/06/2016	Jayaseelan J	Policy Document Reviewed & Updated
1.3	15/11/2017	Santhosh S	Policy Document Reviewed
1.4	12/06/2018	Santhosh S	Policy Document Reviewed
1.5	10/07/2019	Santhosh S	Policy Document Reviewed
1.6	09/11/2020	Santhosh S	Policy Document Reviewed
1.7	06/12/2021	Santhosh S	Policy Document Reviewed
1.8	02/12/2022	Santhosh S	Policy Document Reviewed

Reviewed and Approved By

Version	Date	Reviewed by	Approved By	Owner
1.0	01/08/2014	HR Director	Mr. R.Kumar	CISO
1.1	22/06/2015	HR Director	Mr. R. Kumar	CISO
1.2	14/06/2016	HR Director	Mr. R. Kumar	CISO
1.3	15/11/2017	HR Director	Mr. R. Kumar	CISO
1.4	12/06/2018	HR Director	Mr. R. Kumar	CISO

1.5	10/07/2019	HR Director	Mr. R. Kumar	CISO
1.6	09/11/2020	HR Director	Mr. R. Kumar	CISO
1.7	06/12/2021	HR Director	Mr. R. Kumar	CISO
1.8	02/12/2022	HR Director	Mr. R. Kumar	CISO

1. PURPOSE

Information Security supplier 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 this policy with supplier relationship an information security management system (ISMS) that covers all the processes required to protect information. As per A.15 Supplier releationship requirement.

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.

Information Security in supplier relationship

- To ensure protection of the organization's information that is accessible by suppliers
- To Ensure Information security policy for supplier relationships: Information security requirements for mitigating the risks associated with supplier access to organization's information or information processing facilities shall be documented
- To Ensure addressing security within supplier agreements: All relevant information security requirements shall be established and agreed with each supplier that may have access to, process, store, communicate or provide IT infrastructure components for the organization's information
- To Ensure ICT supply chain Agreements with suppliers shall include requirements to address the information security risks associated with Information and Communications Technology services and product supply chain.
- To Ensure Monitoring and review of supplier services: Organizations shall regularly monitor, review and audit supplier service delivery
- To Ensure Managing changes to supplier services Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks

Business Integrity

- Compliance with Laws

- Conflicts of Interest
- Gifts and Entertainment
- Privacy and Information Security
- Business Resumption and Contingency Planning
- Outsourcing and Subcontracting
- Respect and Diversity
- Discrimination, Harassment and Child Labour
- Working Hours and Wages
- Health and Safety
- Environment

4. RELATED Documented Information's

Access Control Policy
Acceptable Use Policy
End user Computing Policy
Media Disposal Policy
Physical Security Policy
Risk Assessment Policy
Software Licensing Policy
AELData_Supplier Code of Conduct document

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 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.