Third Party Access 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	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

1. PURPOSE

Vendors play an important role in the support of hardware and software management to meet IT operational and capacity enhancement requirements at AEL Data.

The purpose of AEL Data Vendor Access Policy is to establish the rules for vendor access to AEL Data IT Resources, vendor responsibilities, and protection of AEL Data information.

2. SCOPE

AEL Data Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

3. ROLES AND RESPONSIBILITIES

All users using the AEL Data network and resources must adhere to this policy.

4. REFERENCE STATEMENTS

4.1. All third party resource must fill in the authorization form available with the IT Services Support Desk.

4.2. Third party resource must comply with all applicable AEL Data policies, practice standards and agreements, including, but not limited to:

- Privacy Policies
- Security Policies
- Auditing Policies
- Software Licensing Policies
- Acceptable Use Policies

4.3. Vendor agreements and contracts must specify:

- The AEL Data information resource to which the vendor should have access.
- How AEL Data information will be protected by the vendor?
- Acceptable methods for the return, destruction or disposal of AEL Data information in the vendor's possession at the end of the contract

4.4. The Vendor must only use AEL Data information and Information Resources for the purpose of the business agreement.

4.5. Any other AEL Data information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others

4.6. AEL Data will provide an IT point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.

4.7. Each vendor must provide AEL Data with a list of all employees working on the contract. The list must be updated and provided to AEL Data within 24 hours of staff changes.

4.8. Each on-site vendor employee must acquire a AEL Data identification badge that will be displayed at all times while on AEL Data premises. The badge must be returned to AEL Data when the employee leaves the contract or at the end of the contract.

4.9. Each vendor employee with access to AEL Data sensitive information must be cleared to handle that information.

4.10. Vendor personnel must report all security incidents according to the IT Incident Management Policy

4.11. If vendor management is involved in AEL Data security incident management the responsibilities and details must be specified in the contract.

4.12. Vendor must follow all applicable AEL Data change control processes and procedures.

4.13. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate AEL Data management. All vendor maintenance equipment on the AEL Data network that connects to the outside world via the network, telephone line, or leased line, and all AEL Data Information resource vendor accounts will remain disabled except when in use for authorized maintenance.

4.14. Vendor access must be uniquely identifiable and password management must comply with the AEL Data Password Policy and Admin/Special Access Policy. Vendor's major work activities must be entered into a log and available to AEL Data management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

4.15. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to AEL Data or destroyed within 24 hours.

4.16. Upon termination of contract or at the request of AEL Data, the vendor will return or destroy all AEL Data information and provide written certification of that return or destruction within 24 hours.

4.17. Upon termination of contract or at the request of AEL Data, the vendor must surrender all AEL Data Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized AEL Data management System.

4.18. Vendors are required to comply with all State and AEL Data auditing requirements, including the auditing of the vendor's work.

4.19. All software used by the vendor in providing service to AEL Data must be properly inventoried and licensed.

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. EXCLUSIONS

There are no exclusions to the above guidelines

7. ENFORCEMENT

Violation of this policy may result in disciplinary action.