User Account Management 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

To provide guideline for an effective usage of the IT system, by adapting a suitable user management process.

2. SCOPE

The scope of this policy includes system administrators who are in charge of managing user accounts

3. RESPONSIBILITIES

The responsibility of effective implementation of this policy lies with IT & IS Head.

4. REFERENCE STATEMENTS

4.1. Access to multi-user information services would be controlled through a formal user registration process
4.2. A unique user IDs must be given to all users employees, contractors, consultants, temporaries, and other workers at AEL Data, including all personnel affiliated with third parties
4.3. Users are responsible for their actions.
4.4. The use of group IDs should only be permitted where they are suitable for the work carried out
4.5. Group IDs must be approved by functional head.
4.6. Checking that the user has authorization from the system owner for the use of the information system or service. Separate approval for access rights from management may also be appropriate

4.7. Checking that the level of access granted is appropriate to the business purpose and is consistent with Company's security policy, e.g. it does not compromise segregation of duties
4.8. Users must be given a written statement of their access rights
4.9. Users are required to sign statements indicating that they understand the conditions of access as per the HR Procedure..
4.10. Ensuring service providers do not provide access until authorization procedures have been completed
4.11. Immediately removing access rights of users who have changed jobs or left Company.
4.12. Periodic checking for, and removing, redundant user IDs and accounts ensuring that redundant user IDs are not issued to other users. Consideration should be given to including clauses in staff contracts and service contracts that specify actions if unauthorized access is attempted by staff or service agents.
4.13. IT Services Desk is responsible for maintaining the documented information's which could reflect all current user's information and the level of access given to the user's at any point of time.
4.14. Any IDs which is inactive for more than 60 days must be disabled.
4.15. It is necessary to inform the HR to include a statement of understanding to each of the condition for access in the Terms & Conditions document.

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

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