Password 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 and Removed Minimum password age from section 4.
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

For adequate protection against unauthorised access, modification, disclosure, or destruction on the Information system

2. SCOPE

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the AEL Data domain, has access to the AEL Data network, or stores any information on the AEL Data servers. These include personnel with their designated desktop systems.

3. RESPONSIBILITIES

The responsibility of effective implementation of this policy lies with all employees who are handling computerised data of AEL Data .

4. REFERENCE STATEMENTS

4.1. All user level passwords must be of at a minimum of at least 8 (Eight) characters in length and a maximum of 14 characters.
4.2. Maximum password age is 90 days.
4.3. Users must not use any of their past 3 passwords.
4.4. Users must use a complex password .

5. USER GUIDELINE

5.1. Users must be responsible for all activity performed with their personal user IDs and must not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
5.2. All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed at least once every three months.
5.3. Passwords shall not be stored in readable form in batch files, automatic logon scripts, software macros, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them.
5.4. Passwords shall not be revealed on questionnaires or security forms.
5.5. The "Remember Password" feature of applications shall not be used.
5.6. Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site.
5.7. If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
5.8. The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

6. CONSTRUCTING A PASSWORD

All user-level and system-level passwords must conform to the following general guidelines described below.

6.1. The password shall contain more than eight characters.
6.2. The password shall not be a word found in a dictionary (English or foreign).
6.3. The password shall not be a derivative of the user ID.
6.4. The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
6.5. The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
6.6. The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
6.7. The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# $%^&*()_+|~-=\`{}[]:";'<>?,./).

7. COMPLIANCE

7.1. Audits will be performed on a regular basis by authorized organizations/designated officers of AEL Data.
7.2. Audits will be managed in accordance with the Information Security Audit Procedure.
7.3. Every Effort will be made to prevent audits from causing operational failure or disruptions.

8. EXCLUSIONS

There are no exclusions to the above guidelines

9. ENFORCEMENT

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