Data Retention 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 • Tape name added in 4.1 and 5.3
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	S.Santhosh	Policy Document Reviewed
2.2	12/06/2018	S.Santhosh	Policy Document Reviewed
2.3	10/07/2019	S.Santhosh	Policy Document Reviewed
2.4	09/11/2020	S.Santhosh	Policy Document Reviewed
2.5	06/12/2021	S.Santhosh	Policy Document Reviewed
2.6	02/12/2022	S.Santhosh	Policy Document Reviewed
2.7	02/12/2022	Muthukrishnan 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	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
2.7	05/12/2023	HR Director	Mr. R.Kumar	ISH

1. PURPOSE

The Purpose of this policy is to provide a set of guidelines to archive information for special purpose when comes under litigation or criminal investigation and setting up guidelines to destroy the information when the time limit exceeds.

2. SCOPE

This policy applies to IT Services Support Desk under the AEL Data domain to retain business Data and all security logs such as Firewall, IPS, Access control, Active Directory (Security Logs) and Anti Virus (Security Logs).

Any email that contains information in the scope of the Business Record Keeping process should be treated in the retention scope.

3. ROLES AND RESPONSIBILITIES

System Administrator is responsible for keeping a track all the Data being archived within AEL Data Network.

4. REFERENCE STATEMENTS

4.1. Data Retention

1. All Users and Business Data must be stored live for at least a period of one year.
2. IT Services Support Desk is solely responsible to manage this function.
3. All Security Logs such as Firewall, IPS, Access Control, Active Directory (Security) and Antivirus needs to be stored live for a least duration of one year.
4. Furthermore all security logs must be archived on CD's / DVD's & Tapes for another one year.

5. COMPLIANCE

5.1. Establish a record of all compliance task force, so there are easily identifiable “go-to” people regarding retention activities.
5.2. The compliance task force should create detailed logs of record-purging and back-up activities.
5.3. Archiving procedures should be periodically reviewed and tested. If back-up CD’s / DVD’s & Tapes hardware is updated, be sure that there’s a back up plan for accessing date on old CD’s & DVD’s Those likely will not work with newer hardware. All back-up tapes should be stored in a safe place.
5.4. Make certain that all media are considered and accounted for use within this policy. This includes not only servers, desktops, and laptops, but also PDAs, BlackBerries, and various removable media devices.
5.5. It’s a good idea to have an objective third party periodically review and validate that policies are being followed. In doing so, the vendor should interview key personnel and review a sampling of data using forensic tools.

6. EXCEPTIONS

There are no exceptions to the above guidelines. Unless required for a specific application / purpose, this must be approved by CISO in writing

7. ENFORCEMENT

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