Backup 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	27/06/2014	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 identify the need of fault tolerance, backup protects against loss of data due to Hardware / Software failure and human error.

2. SCOPE

The guidelines for Back up extend to all employees and systems of AEL Data who are handling computerised data.

3. ROLES AND RESPONSIBILITIES

The responsibility of effective implementation of this policy lies with Information Security Head & IT Dept.

4. REFERENCE STATEMENTS

4.1. Backups

The policy mentioned above is a broad policy applicable to business critical data as well as configuration information stored on network devices on the corporate network. The detailed guidelines for all equipments, needs to be prepared depending upon the function.

4.2. Storage of backups

Finding a good way to store backups is almost as important as creating them. Backups, installation media and boot disks should be stored in a place where only authorized people have access to them. In order to make restorations simple, backups need to be well labelled. Labelling

includes clearly marking the media itself as well as including a table of contents so that individual files on the CD's, DVD's , External HDD's & Tape Cartridges can be located easily. In sites where several people share the responsibility of taking backups or a number of different commands are used to create backups, the label should also include the commands used to create the backup.

Most backup media are sensitive to heat, humidity, direct sunlight and dust. So it is imperative that they should be stored in a cool, dry space. Keeping backups in the same room as the servers may be convenient but not advocated. If the said room is struck with a disaster the backup media could also be destroyed.

4.3. Offsite backups

To ensure the availability and access to the AEL Data data files following a disaster, copies of the files must be stored in a location separate from where the data files are normally preserved. This off-site storage is applicable to data files which are used on a regular basis in conducting business as well as those which must be retained to meet the requirements of the legislation and other regulations in force regarding retention of AEL Data Documented information's.

Information Security Head and Information Security Committee should review existing and potential off-site storage facilities to determine the protection, which should be provided to the data stored at such locations. This review should address environmental, physical and procedural security issues directly related to the facility and handling and the movement of media.

There should be a system for taking off-site storage of all back up media as well as entrusting the responsibility of regular preservation of off-site back up media by framing appropriate procedures.

4.4. Retrieval

Backups taken should be periodically tested for retrievability/recoverability of information. But this should never be tried in a 'live' area for it could result in loss of live data. This should be done on a monthly basis.

4.5. Backup before and after update

A complete backup of the equipment must be done before and after a major update. The backup taken before the update can be used as a back out procedure in case the update fails.

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 failure or disruptions.

6. EXCEPTIONS

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

7. ENFORCEMENT

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