Policy Domain	**Backup & Recovery Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Document Control			
Prepared By **Vineet Kumar Chawla** **(Sr. Consultant IT)**	**Reviewed By** **Maruti Divekar** **(IT Head)**	**Checked By** **B P Rauka** **(CFO)**	**Approved By** **Mukund Kabra** **(Director)**

Document Modification History

SR #	Document	Version No.	Reviewed On	Checked On	Approved On	Effective Date	Authorized Signatory
1.	Backup & Recovery Policy	1.0	05TH Mar 21	10th Mar 21	10th Mar 21	11th Mar 21	
2.							
3.							

Document Control

- This document is subject to version control and shall be managed by IT Head. Any request for amending this document shall be approved by Director. The IT Head shall review this document at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes.

- The document is available on Helpdesk Portal under Announcement and Server shared folder under AETL Policies and provided with HR Joining Kit, in non-editable pdf format and all the employees are expected to read and adhere to it. The approved and signed copies are available with IT Team, which can be used for audit purpose only. IT Team is responsible for maintaining updated copy of this document and its effective communication within Advanced Enzymes (AETL).

Policy Domain	**Backup & Recovery Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

1. Overview

This Procedure defines the backup procedure and recovery procedure for servers, network devices, end user systems, storage which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the application server, and the Database server.

2. Purpose

The purpose of this policy is to safeguard the information assets of AETL and to prevent the loss of data in the case of an accidental deletion or corruption of data, system failure by enabling secure backup and restoration processes on the media employed in the process.

3. Scope

This policy will be applicable to recovery and backup of all critical business data. This policy refers to the backing up of data that resides on servers, individual PCs and laptops. All users need to keep their data on server provided storage only except roaming laptop users. It is imperative that end-users save their data to the appropriate server provided storage only, in order that their data is backed up regularly in accordance with company regulations and backup policy. Roaming laptop users can keep their data on laptop and need to take monthly backup on provided network attached storage path outlined in this policy. Users does not need to transfer their server storage data that is saved on a network or shared drive, as these are backed up when the servers are backed up, as per our backup policy. IT team will be responsible for backing up server's data as per backup policy schedules and local Laptop/Desktops data backup need to take every Month by the individual users with the help of IT person.

4. Policy

The IT department recognizes that the backup and maintenance of the data for all file servers, PCs are critical to the viability and operations of the company. It is essential that certain basic standard practices be followed to ensure that data are backed up on a regular basis.

Backup policy applies to all equipment which has the capability of storing data and is not limited to Servers, DB and Applications. The backups of all such equipment's will be done on tape storage thru automated backups.

4.1 Backup Process

Servers : All the server data should be backed up to storage on or before 7th of every month. This will be used to restore the server failure. The following physical/virtual servers configured to backed on or before 7th of every month.

Network Devices

All the configurations of network devices i.e. Fortigate firewall, L2 Switches, Routers (AETL Owned) etc. to be backed up on central storage.

Laptop/Desktop devices: - It's the responsibilities of employees to copy the data from laptops/desktops to central storage which will be provided and maintained with IT department.

The following process to be followed for back up of the data:

Onsite Data Backup

1) Daily Full Backup

a. SAP HANA, SAP B1 Server (B1-SQL Database) and Payroll server (SQL Database) will be backed up at AETBACKUP SERVER

Retention Period – 3 days on AETBACKUP Server Storage

2) Weekly Full / Daily Incremental Data Backup

a. File Server Centrally stored shared folder full data backed up on every Saturday and incremental data backup on daily basis on Tape Storage.

3) Monthly Full Data backup

a. File Sever centrally stored share folders data/ payroll database/ Sap HANA DB and Roaming user's data will be taken on or before 7th of every month on Tape Storage.
b. All above Virtual Machines full backup (Bare Metal Level) will be done on or before 7th of every month on Tape Storage.

4) Offsite Data Backup

a. Above monthly backup (Point No. 3) storage tapes will be transferred to other locations for offsite data backup.

5) Storage of Backup Tapes: Monthly full data backup tapes will be kept in alternate locations to overcome any natural disaster.

a. TCO Monthly Full (offsite) data backup tape would be sent to SNF server room.

b. WRC Monthly Full (offsite) data backup disk would be sent to SNF server room.

c. NTRC Monthly Full (offsite) data backup disk would be sent to SNF server room.

Validation of Backup

The following process shall be followed to ensure the stability and accuracy of the taken backup.

a. On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
   1. To check for and correct errors.
   2. To monitor the duration of the backup job.
   3. To optimize backup performance where possible.

b. IT will identify problems and take corrective action to reduce any risks associated with failed backups.

c. Once in a year data restoration test need to be done.

d. IT will maintain records demonstrating the test restores so as to demonstrate compliance with this policy for auditing purposes.

Restoration test of backup:

- On backup server there shall be a folder name “Restore_Testing” in which sample data shall be restored.
- “Restore_Testing” folder has no access to any user other than System administrator.
- The SAP backup shall be restored once in a year on sandbox system to validate the backup.

Storage condition of Backup

All electronic records shall be stored at safe place where there is no impact of Temperature, Humidity, High voltage, Electromagnetic field etc.

The electronic records shall be kept in the lock and key so as restrict any alteration or deletion of the data in electronic form.

Backup tapes management and transportation:

- All backups shall be written on tape media with capacity of minimum 400 GB or above compatible capacity.
- Media will be clearly labeled and stored in a secure area that is accessible only to IT staff or employees of the contracted secure off-site location used by IT.
- During transport or changes of media, media will not be left unattended.

Media will be retired and disposed of as described below:

Prior to retirement and disposal, IT will ensure that:

- The media no longer contains active backup images.
- The media's current or former contents cannot be read or recovered by an unauthorized party.
- With all backup media, IT will ensure the physical destruction of media prior to disposal.

Data Recovery

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 1-2 working day if the destroyed equipment has been replaced by that time.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 8-16 working hours on based on user request and approval from his HOD or Management.

5. Restoration Requests

In the event of accidental deletion or corruption of information (data), requests for restoration of information (data) should be raised on helpdesk portal with cc to their reporting manager (HOD) and IT Head.

6. Roles & Responsibility Matrix (RACI)

Role Activity	IT Head	ISMS Steering Committee	Internal Users	External Users	Exempted
Authoring of this document	RA	RA	-	-	-
Approval of this document	I	CI	-	-	-
Sign-off of this document	CI	CI	-	-	-
Application of this document	RA	RA	RA	RA	-

R	Responsible
A	Accountable
C	Consulted
I	Informed

7. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Data/Configuration integrity loss,
- System crash and avoidable interruptions,
- Security failures,
- Confusion/delay in system configuration,
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Backups are done on regular interval.
- The restorations are scheduled to ensure planned results.
- All backup logs are monitored on daily basis.
- If any issues are noticed in Backup logs, Backups are rescheduled.

8. Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any.

IT Head will be responsible for reviewing the policy and communicating the changes made therein.

9. ISMS Steering Committee Members

1. Mukund Kabra (Director)
2. B. P. Rauka (CFO)
3. Maruti Divekar (IT Head)

10. AETL IT Helpdesk Contact Details

- Logging an online support request: http://192.168.2.7:8080
- Email: it.helpdesk@advancedenzymes.com
- Telephone: 022 41703234