Policy Domain	**IT Business Continuity Plan**	**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.	IT Business Continuity Plan	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	IT Business Continuity Plan	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

Policy Domain	**IT Business Continuity Plan**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

1. Overview

Business continuity planning (BCP) is the process a company undergoes to create a prevention and recovery system from potential threats such as natural disasters or cyber-attacks. BCP is designed to protect personnel and assets and make sure they can function quickly when disaster strikes.

2. Objective

A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. The importance of IT BCP plan is to ensure business continuity on the occurrence of following risks:

- Risks associated with Natural disasters of all types
- Extensive downtime of mission critical IT applications
- Accidents such as fire, explosions etc. which could damage IT infrastructure
- Sabotage, both internal and external
- Power outages
- Communication failure
- Disruptions in transportation due to various factors, preventing employees from attending work
- Security issues that can bring down the network
- Environmental disasters
- Cyber-attacks on the business by hackers

3. Applicability and Scope

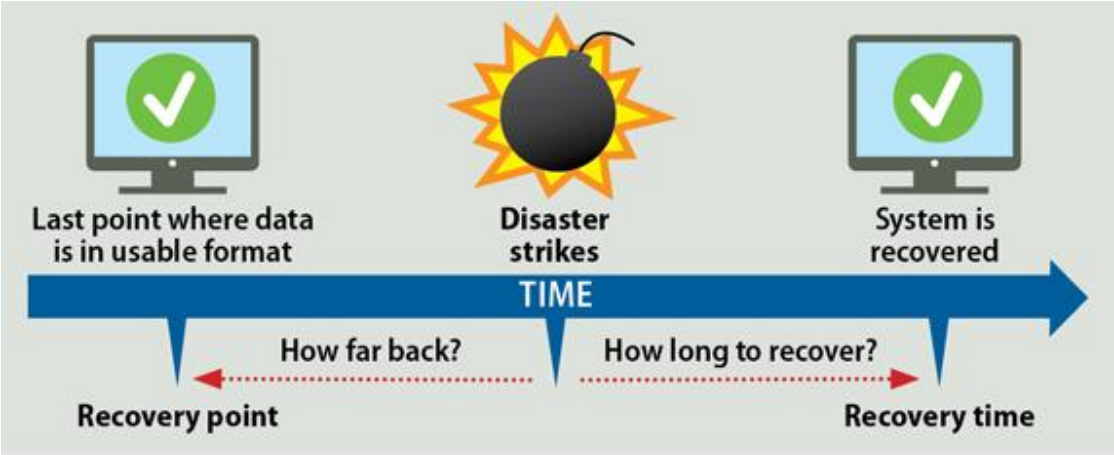
This procedure is applicable to all information and info processing assets, employees and third parties of Advanced Enzymes (hereafter referred as “AE”)

Any exception to this policy should be routed and approved by Management.

4. Definitions

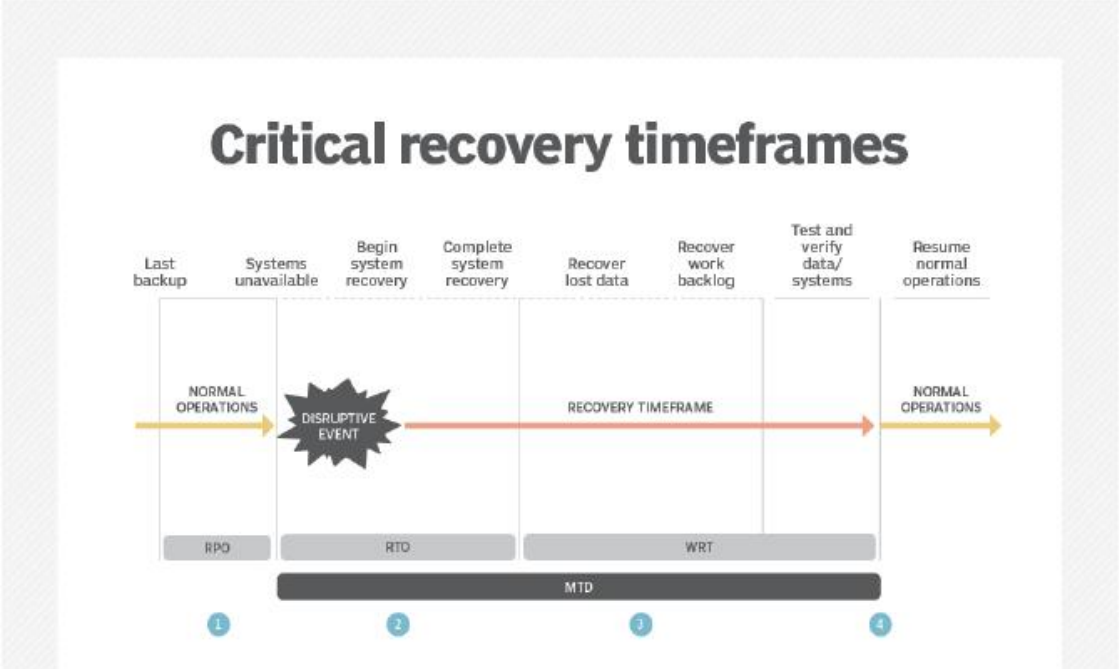
a. Recovery Time Objective (RTO)

It refers to the maximum acceptable amount of data loss a critical application can undergo before causing measurable harm to the business. It is also interpreted as the maximum amount of time the concerned service can be down following an incident before normal operations are back online.



b. Recovery Point Objective (RPO)

It marks the age of backup files an organization must recover to resume normal operations following an incident. In other words, it stats how much downtime an application experiences before there is a measurable business loss.



Point 1: Recovery Point Objective. The maximum sustainable data loss based on backup schedules and data needs.

Point 2: Recovery Time Objective. The duration of time required to bring critical systems back online.

Point 3: Work Recovery Time: The duration of time needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered)

Points 2 and 3: Maximum Tolerable Downtime. The duration of RTO plus the WRT

Point 4: Test, verify and resume normal operations.

5. Business Continuity Plan Coverage

5.1 Business Continuity Plan covers following sections in detail.

- BCP Governance
- Business Impact Analysis
- Business Continuity Process/Procedures
- Readiness to Implement BCP
- Testing and training of BCP

5.2 BCP Governance Committee

BCP Committee will be in-charge of defining/revising/coordinating/executing BCP plan. BCP committee members are listed below:

- Director
- CFO
- Head IT
- IT Administrators
- Head - Admin
- Head - HR
- Functional Heads

5.3 Business Impact Analysis

The critical business from an IT BCP perspective are listed below:

Service Name	Impact Rating*
Core SAP S/4 HANA System	8
Email Services	7
Internet/MPLS Connectivity Services	6
Server Data	4

*Higher numerical value represents more critical service. 8 being highest Priority, 1 being lowest priority.

Guidance in accessing probability, impact and control rating associated with risk are given below

	Factors	Expectation over value Range				
I	Probability	Very High	High	Medium	Low	Very low
		Certain to happen sometime in next 12 months	Highly likely to happen sometime in next 3 years	Likely (or possible) to occur at some time in the future		
ii	Impact Rating	Very high	High	Medium	Low	Very Low
iii	Control Rating	Excellent	Very Good	Good	Medium	Poor
V		Effective and efficient	Reasonable, well balanced and effective	Reasonable and well balanced	Just starting	Very few mechanisms are in place

6. Business Continuity Procedure

Business Continuity Procedure

Backup plan & BCP for the critical services is defined and executed at defined frequency as per the below table(s).

6.1 Core System SAP :

Backup Plan

Step No	Activity/Work Shop	Frequency	Responsibility
1	Physical backup (including data files, control files, log files, executables) of production (Application Server) to be taken	On or before 7th Every Month	IT Team
2	Physical Backup (including data files, control files, log files, executables) of production (Database Server) to be taken	On or before 7th Every Month	IT Team
3	Full Database Backup on AETBACKUP Server	Daily	IT Team

BCP (Business Continuity Plan)

In case of any events occurred, after seeking ISMS committee approval, IT team will execute following plan:

Step no.	Event	Activity/Work Step	Time metrics	Responsibility
1.	SAP Apps server OS is corrupt / Server Down	1) Since APPS server on virtual host AETAPPVS01 and AETAPPVS02 are in VM, the load will shift to one of the other server. 2) Restore full machine backup or Create VM, Reinstall the OS and move the APPS server back to Original Apps server.	**RTO: 16 hrs** **RPO: 8 hrs**	**IT Head**
2	HANA Database Server OS is corrupted/ Server Down	1) Since SAPPRDDB & SAPNPDB PRD DB are in sync the load will shift to failed over server. **2)** Restore full machine backup or Reinstall the OS, re-configure the server from backup and move the DB server back to Original DB server **&** configure Sync.	**RTO: 16 hrs** **RPO: 8 hrs**	**IT Head**
3	Data Center is not available	If primary Hosted environment is down, then secondary DR site (DR-Sinnar) hosted will be made available.	**RTO: 8 hrs** **RPO: 4 hrs**	**IT Head**

6.2 Email Services – Google Workspace – SaaS Model

Backup Plan:

Step No.	Activity/ Work Step	Frequency	Responsibility
1	Vendor maintains 1 site with one DR and real time replication of data	Near Real Time	Google

BCP (Business Continuity Plan)

Step No.	Event	Activity/Work Step	Time Metrices	Responsibility
1	Cloud Instance is corrupt/Server down	If primary Cloud Hosting environment is down, then automatically secondary (DR) Cloud environment will be made available by Email Provider.	RTO:6 hrs RPO:1 hrs	Cloud Hosting Company (Google)
2	Email data corrupt / missing for downloaded emails	Recover selected data from Google server	RTO:3hrs RPO:3hrs	Cloud Hosting Company (Google)

6.3 Internet/MPLS Connectivity Services

Backup Plan:

Step No.	Activity/ Work Step	Frequency	Responsibility
1	Each site having redundant internet connectivity	Near Real Time	IT Team
2	In case of MPLS failure IPsec VPN configured to access required resources over internet	Near Real Time	IT Team

BCP (Business Continuity Plan)

Step No.	Event	Activity/Work Step	Time Metrices	Responsibility
1	**Internet Connectivity down / failure**	**Switch to secondary ISP line**	RTO:5 Mins RPO:5 Mins	IT Team
2	**MPLS Connectivity down / failure**	**Switch to IPSec VPN over internet**	RTO:5 Mins RPO:5 Mins	IT Team

6.4 Server Data

Backup Plan:

Step No.	Activity /Work Step	Frequency	Responsibility
1.	**Weekly Full & Daily Incremental data backup on Tape and disk**	**Daily**	**IT Team**
2.	**Full data backup on Tape (sent to alternate location)**	**Monthly**	**IT Team**

BCP (Business Continuity Plan)

In case of any events occurred, after seeking Dept head/IT Head/ISMS committee approval, IT team will execute following plan:

Step No.	Event	Activity /Work Step	Time Metrices	Responsibility
1.	**Server network share folder data, SQL DB, HRMS application Server is corrupt/Down**	**Restore data from latest available backup at site / Recall the tapes from alternate location and restore**	**RTO : 8 hrs RPO : 4hrs**	**IT Team**

6.5 BCP of other allied Services

Step No.	Event	Activity /Work Step	Time Metrices	Responsibility
1.	**Firewall at corporate gets corrupted/ hardware failure**	**Lodge complaint with service provider**	**RTO : 24 hrs RPO : 2 hrs**	**IT Team**
2.	**L2 Switch at corporate gets corrupted/ hardware failure**	**Standby switch will be replace / Lodge complaint with service provider**	**RTO : 24 hrs RPO : 15 min**	**IT Team**
3.	**Server hardware failure**	**Lodge complaint with OEM**	**RTO : 3 days RPO : 24 hrs**	**IT Team**
4.	**Catastrophic failure/ Natural calamity at HO office (including Local Data center down, electrical**	**Core IT systems SAP will be accessible at SNF & email will still remain available over public internet.**	**RTO: 4 hrs RPO: 1 hrs**	**IT Team**

	failure, LAN down, Local infra not available)	**Remaining employees can continue work from respected locations.**		
5.	**Cyber Attack**	**Cyber Crisis management plan will be activated**	**RTO: 48 hrs RPO: 24 hrs**	**Management**
6	**Sabotage or damage of IT assets**	**IT asset inventory is maintained comprising of desktop, laptops, printers.**	**RTO :24 hrs RPO;24 hrs**	**IT Team**

7. Testing & Training of DR/BCP

Testing & Training of DR/BCP

S. No.	Testing type	Frequency/Plan
1.	Structured Walkthrough	Every 1 year
2.	Component Testing	Every 1 year
3.	Integrated simulation/ Full operations test	Every 1 year

Three distinct type of test levels are identified to help validate BCP accuracy & effectiveness.

Structured walkthrough:

It is also referred as "table top" exercise, the structured walk-through is a paper evaluation of a BCP/DR designed to expose errors or emissions without incurring the level of planning and expenses associated with performing a full operations test. It is in effect, a role playoff a "disaster" scenario that takes place with the confines and safety of conference room.

Component testing:
It is the physical exercise defined to assess the readiness of discrete plan elements and recovery activities. The isolation of key recovery activities allows team members to focus their efforts while limiting testing expense and resources. This methodology is effective for identifying and resolving issues that may adversely affect the successful completion of a full operations test.

= Components test include:
- Evacuation test
- Emergency notification test
- Application recovery test
- Remote or Dial-in access test
- Critical business function recovery test

Integrated Simulation/Full operations test:
The full operations test requires extensive planning and preparation and should not be performed until most, if not all, of the plan components have been tested. This test requires the simulated recovery of critical business functions across a business unit

8. Maintenance & Review of BCP

The BCP will be reviewed on occurrence of following triggers (not limited to):

- Regulatory requirements
- New critical services introduced.
- New major hardware/technology platform change
- Major IRR incident impacting BCP effectiveness
- Vendor bankruptcy
- Facility movement
- Personnel changes / relocation
- Transfer of functions
- Consolidation of outsourcing of functions
- Change in critical third-party vendors/suppliers
- Results of BCP testing

The BCP plan will be reviewed on yearly basis to ensure that all required updates are captured.

9. 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

10. Risk for Non-Compliance

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

- Business Loss,
- Data corruption,
- System crash and avoidable interruptions,
- Security failures,
- Loss of unavailability of important data
- Integrity and reputation loss

Compliance with this policy initiates the following key controls:

- Confidence of customers and stake holders as the organization is ready to face any technological disruptions.
- All IT equipment up with minimum loss of data
- Any issues noticed during testing are controlled.

11. ISMS Steering Committee Members

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

12. AETL IT Helpdesk Contact Details

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

13. Annexure A – Supporting templates

Sr.No	Template Name	Template
1	**Contact list of BCP Members**	
2	**Contact list of Vendors**	
3	**Escalation Matrix of Vendors**	
4	**Contact list of Alternate sites (SNF)**	