

<b>Document Name</b>	<b>Business Continuity and Disaster Recovery Plan for CSE &amp; CCMLP</b>
<b>Document Creation Date</b>	<b>25/03/2021</b>
<b>Document Created By</b>	<b>CISO-CSE</b>
<b>Version Control History</b>	<b>1.5</b>
<b>Document Reviewed Date</b>	<b>05/12/2024</b>
<b>Document Reviewed By</b>	<b>CISO-CSE &amp; CRO-CSE</b>
<b>Document Approved By</b>	<b>Standing Committee on Technology</b>

## **CSE's Business Continuity and Disaster Recovery Plan**

### **General Overview**

When disaster strikes, business suffers. A goal of business planning is to mitigate disruption of product and services delivery to the greatest degree possible when disruption due to disaster occurs. Business continuity is the overarching concern.

An IT disaster recovery plan is the lynchpin of an overall business continuity strategy. And the purpose of business continuity is to maintain a minimum level of service while restoring the organization to business as usual. If a business fails to put a disaster recovery plan in place then, when disaster strikes, the company risks losing customers to competitors, losing funding and having the need for its products or services re-evaluated and deemed unnecessary.

### **Information Technology Statement of Intent**

This document delineates the policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes the recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

The mission is to ensure information system uptime, data integrity and availability, and business continuity.

### **Objectives**

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

### **Critically Important IT Devices**

There are several critically important items in the Exchange like:

1. Tandem Servers to run the CSTAR Trading application, the main trading system of CSE's own Trading Engine.
2. Core Switches to maintain the connectivity to all the servers with users through LAN and WAN

3. Router & Firewall used at the DC (Data Centre) to provide access of IT Resources to the end users
4. Communication Links commissioned through different ISPs at the DC to provide access of IT Resources to the end users
5. Air conditioning System of DC
6. Intel Servers used in Section-13 arrangement to trade in NSE and BSE
7. UPS System to provide power to the infrastructure uninterruptedly
8. Generators to provide backup power in case of power failures

## **Maintaining Critical IT Asset Register**

All the hardware/device mentioned above should be recorded in a register called “Critical IT Asset Register” which is needed to comply SEBI’s Cyber Security audit compliance. It is needed to get immediate hands on information about the critical asset which would be required in case of any emergency situation happens or any cyber security threat/incident occurs for immediate detection and its proper remedial actions thereof.

But after the closure of CSTAR Trading in 2014 and subsequent closure of Section-13 arrangement in 2023 the critical assets became abundant and unused. Hence the importance of register became irrelevant. Only some non IT assets or devices like DG Sets, UPS and some few desktops & a server in CCMPL DP remained active on date and they have remained in the register and still considered as critical IT assets.

## **BCP and DR Plan for Tandem System:**

CSE runs Trading system CSTAR through main frame TANDEM servers. The servers are Single Level Fault Tolerant System guarantying 99.98% system availability. It’s a time tested stable system giving 100% fault tolerance at least to CSE since 1996 till date. No failure has been observed.

However to tackle any kind of natural calamity which is like fire, earthquake etc. CSE maintains a backup server which is predominantly used as development and test environment and during MOCK drills.

In first step if any disruption occurs to main trading servers the trading can be re started within 30 minutes from the Backup server which is also a fault tolerant system.

As the Trading Engine in CSE is nonoperational since 2013, the need for DR site does not arise here. However whenever Trading in CSE restarts CSE will comply with SEBI’s guidelines and restart their trading system with proper DR site in place.

## **BCP and DR Plan for Core Switches:**

CSE has two HP made Core Switches which is the main backbone of the LAN network connecting all the Servers, Members, CSE operators, WAN members to connect through it to access trading system.

As two switches are configured in failsafe mode, the first level of fault tolerance is achieved. In case of any exigency HP to be connected for immediate fault booking and resolution of the hardware failure. TCS monitor and maintain the whole CSE Network and the detection of any fault is observed by them only and they take care all the call booking with OEM till resolution of the problem.

If any disruption occurs to any of the Core Switches the other switch which is configured in failsafe mode would automatically takeover at real-time mode. The Switches are with lifetime warranty with the OEM and for any hardware failure it would be immediately repaired. TCS takes care of the AMC matter with OEM.

### **BCP and DR Plan for Router & Firewall:**

CSE had two Fortinet made 80C Firewall Routers which are used in LAN network as firewall for maintaining outside internet security to trading system and internal users.

As two firewall Routers are configured in failsafe mode, the first level of fault tolerance is achieved. In case of any exigency Fortigate to be connected for immediate fault booking and resolution of the hardware failure. Odyssey Computer Services Pvt. Ltd. maintain the Firewall devices and the monitoring of the Firewall is done by TCS Ltd. The detection of any fault is observed by TCS Ltd. only and they take care all the call booking with OEM till resolution of the problem.

If any disruption occurs to any of the Firewall router the other switch which is configured in failsafe mode would automatically takeover at real-time mode. The routers are with AMC with the OEM through Odyssey Computer Services and for any hardware failure it would be immediately repaired while the other is in operation till that time the faulty one is get repaired.

### **BCP and DR Plan for Communication Links Commissioned through different ISPs at the Data centre:**

CSE has many of communication links from different ISPs terminated and commissioned in the Data Centre for different usage like CSE's Own VPN system for members and for trading in NSE and BSE (from the exchanges for trading terminals) etc.

Three links from Tata, Airtel and Sify are used for VPN solution for the members. Dual connectivity for NSE and BSE trading from the exchange (point to point leased circuit connectivity) is used. The links are maintained directly by the ISPs providing various links of different bandwidth.

If any disruption occurs to any of the links, we get notifications through mail for VPN solution and for Exchange connectivity problem it is intimated through the exchange. We register call to the particular ISP for resolution of the problems and resolved at the earliest. The emergency contact for the call booking of different ISPs are provided. As all the links have backup links for any particular usage, the BCP and DR plan is resolved.

### **BCP and DR Plan for Air Conditioning System in Data Centre:**

CSE has central Air Conditioning system installed for its Data Centre at the Mezzanine Floor of the Exchange at 7, Lyons Range, Kolkata 700001.

If any disruption occurs to the air conditioning system, in-house 24x7 electrical as well as AC operators takes care of the fault.

For DR, CSE have separate two Split ACs installed in the Data Centre for exigency as well as using them at extreme heat generation whenever observed.

## **BCP and DR Plan for Servers used in Section-13 Arrangement:**

There are 13 Intel based Servers in Section-13 Arrangements. Out of that at present Three Servers are used for ODIN multi exchange trading software to run NSE and BSE trading applications which is Online and real time basis trading activities for the trading time. These servers can be treated as Critical servers. Rest are used offline purposes like UAT, FTP, CLASS Back office and other use.

At the time of failure of any server the UAT server for ODIN is configured in such a manner that if Application Server is down then the UAT server could be connected as application server just with a change of IP address and it would continue to work. Same case for Database server as well.

As CSE regularly takes part in DR drills and Mock Trading of both the other Exchanges like NSE and BSE, the DR site is not necessary. However CSE use web trading of BSE and NSE and in case of any hardware exigency and trading disruption happens locally to Section-13 arrangement, all the Members who trades in Section-13 arrangement are registered with the NSE and BSE web trading platform and they can directly login to their respective IDs and trade from there as a part time solution immediately.

## **BCP and DR Plan for iBOS Servers used in CSE Back-office:**

There are 2 Intel based Servers used in iBOS back office application. One Windows based server is used as Application Server and one Linux based server is used as Database server having Oracle as database software.

There is no fallback server present at the moment. All the software backup and database backup are taken on weekly basis and if any changes are done in mid of week. The daily backup is taken of software and database in local media (server itself). The database is backed up in application server for extra safety. The external media containing backup are stored in accounts department and ITD simultaneously.

At the time of failure of any server, the AMC vendor is contacted for immediate repair and starting of server and application at the earliest possible time.

## **BCP and DR Plan for DP Servers used in CCMPL DP:**

There are 2 Intel based Servers used in CCMPL DP operation including NSDL & CDSL. One Windows based server is used as NSDL local Server and One Window based server is used as DP Back-office server having SQL Server as database. For CDSL data resides in the CDSL central database server and CCMPL only operates through web based client machine only.

There is no fallback server present at the moment. NSDL daily data is backed up as per NSDL prescribed procedure daily and kept in two sets local and remote basis. Back-office server data is backed up also daily in local disk and taken in USB HDD weekly basis.

At the time of failure of any server, the AMC vendor is contacted for immediate repair and starting of server and application at the earliest possible time.

## **BCP and DR Plan for Central UPS:**

CSE have two 80KVA UPS installed in HA mode to power CSE IT infrastructure. These Tata Liebert UPS are capable to serving all the power requirement of IT Infra. These are maintained by OEM, VERTIV Ltd.

In case of any failure the alternate UPS can take care of the load till it is repaired. Comprehensive maintenance is provided by the OEM and immediately it would be repaired.

In case of both the UPS fails then CSE have another set of Two 60KVA UPS installed and used for internal office use which can be used for providing power to IT infra in case of extreme exigency.

### **BCP and DR Plan for Generator Sets:**

CSE uses three 125KV generators alternatively whenever any power cut happens. Any two sets are required to run to backing up the total power requirement of the Exchange. In night only one Set is enough to provide adequate load of nonstop IT infra.

As all the three sets are on regular maintenance and monitoring the possibility of breaking down of all three sets at a time is practically impossible other than any unnatural calamity like building fire or building collapse.

For any other exigency the maintenance department takes care of its maintenance and report.

### **Types of Disaster Observed in Area**

In Kolkata earthquakes and not in high Richter scale due to soft soil nature in Gangetic riverside cities like Kolkata.

Fire safety arrangements have been implemented with proper alarm system in place and its regularly monitored 24x7 by electrical maintenance personnel.

Periodic fire drills are done to check all systems are in good order.

### **Failure Modes and Effects Analysis**

FMEA prioritizes failures according to **severity, frequency and detectability**. Severity describes the seriousness of failure consequences. Frequency describes how often failures can occur. Detectability refers to degree of difficulty in detecting failures.

<b>Area</b>	<b>Severity</b>	<b>Frequency</b>	<b>Detectability</b>
Tandem Servers to run the CSTAR Trading application, the main trading system of CSE's own Trading Engine.	HIGH	VERY UNLIKELY	CRITICAL
Core Switches to maintain the connectivity to all the servers with users through LAN and WAN	HIGH	VERY UNLIKELY	CRITICAL
Intel Servers used in Section-13 arrangement to trade in NSE and BSE	HIGH	LIKELY	EASY
UPS System to provide power to the	HIGH	VERY UNLIKELY	CRITICAL

infrastructure uninterruptedly			
Generators to provide backup power in case of power failures	LOW	VERY UNLIKELY	CRITICAL

### Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
1. Tamal Ghatak, Executive	Work	033 4025 3041
	Work Alternate	033 4025 3045
	Mobile	+919432124722
	Home	+918240503003
	Email Address	<a href="mailto:tamalghatak@cse-india.com">tamalghatak@cse-india.com</a>
	Alternate Email Address	
2. P Dutta, CFO	Work	033 4025 3019
	Work Alternate	033 4025 3000
	Mobile	+919836900225
	Home	
	Email Address	<a href="mailto:pdutta@cse-india.com">pdutta@cse-india.com</a>
	Alternate Email Address	
3. Asis Maity, CRO	Work	033 4025 3033
	Work Alternate	033 4025 3000
	Mobile	+919836900216
	Home	
	Email Address	<a href="mailto:asismaity@cse-india.com">asismaity@cse-india.com</a>
	Alternate Email Address	


### External Contacts

Name, Title	Contact Option	Contact Number
1. Ketan Doshi, Odyssey Computer Services	Work	033 2243 4343
	Work Alternate	
	Mobile	9830005500
	Home	
	Email Address	<a href="mailto:ketan@odysseygroup.co.in">ketan@odysseygroup.co.in</a>
	Alternate Email Address	
2. Sahajamal Hossain, Electrical maintenance	Work	
	Work Alternate	
	Mobile	9831034623
	Home	
	Email Address	
	Alternate Email Address	
3. Ajeet Swain, Oritech Computer	Work	9830416101
	Work Alternate	
	Mobile	9830416101
	Home	
	Email Address	<a href="mailto:ajeet@oritechgroup.co.in">ajeet@oritechgroup.co.in</a>
	Alternate Email Address	

### Purpose for contacting internal or external contacts:

Various section of contact persons 'numbers are provided for different types of activities. Tried to have multiple numbers from an external agency/vendor for different jobs.

**Damage Assessment Form**

 <b>THE CALCUTTA STOCK EXCHANGE LIMITED</b> <b>INFORMATION TECHNOLOGY DIVISION</b>		
<b>Key Business Process Affected</b>	<b>Description Of Problem</b>	<b>Extent Of Damage</b>

## **Version Control History**

**Version Change Date: 17/05/2023**  
**Version Number: 1.4**

### **Changes:**

- Heading changed with addition of 'for CSE & CCMP L'
- DR Plan for Core Switches, Central UPS and Generator sets have been included
- BCP & DR Plan for iBOS servers have been included
- BCP & DR Plan for CCMP L DP operations have been included
- The purpose for contacting different internal and external contacts has been mentioned
- Router & Firewall used at the DC (Data Centre) is included in Critically Important IT Devices List
- Communication Links commissioned through different ISPs at the DC is included in Critically Important IT Devices List
- Air conditioning System of DC is included in Critically Important IT Devices Lis
- Corresponding BCP & DR plans for these new three items are added

## **Version Control History**

**Version Change Date: 05/12/2024**  
**Version Number: 1.5**

### **Changes:**

- Inclusion of CRO as reviewer
- Changes in contact numbers of various vendors (removed from the list as all of them is not renewed their maintenance service any more).
- Inclusion of "Maintaining Critical IT Asset Register" section.