(6)

Life Insurance Corporation of India
Staff Co-operative Urban Bank Ltd No.3314

BUSINESS CONTINUITY POLICY – 2024-25

The LIC of India Staff Co-operative Urban Co-operative Bank Ltd No.3314

BUSINESS CONTINUITY POLICY AND DISASTER RECOVERY PROCEDURE

The policy is called the Business Continuity Policy and disaster recovery procedure of The LIC of India Staff Co-operative Urban Co-operative Bank Ltd No.3314 approved by the Board in its meeting held on 15/03/2025 vide Resolution No.IV

The data centers are considered as life-blood of any organization and data centers of today face the challenges of increasing complexity both in terms of technology and its management. The bank rely heavily on the availability of data and any loss in service translates into loss of revenue. There are a lot of indirect costs associated with not having proper arrangements to yield the maximum out of the resources available to the bank.

For service oriented industries down time means not only service unavailability but loss of customer satisfaction which is the most focused area and for banks three things are important that is customers, data and systems. Protecting data and systems is difficult and considered as most prominent factor.

The consequences of disasters for an organization will be:-

a) The number of customers will be decreased
b) Customer relation will be degenerated
c) There will be huge reduction in profit
d) The data loss.

Therefore, today, it is absolutely necessary to have a comprehensive business continuity plan as the general operations are dependent on the systems providing different services to the business units.

A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available.

Business Continuity Plan (BCP) is basically a process of developing advance arrangements that enable the bank to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change, so the benefits of BCP are to increase the quality, productivity and positive customer experience.

The ground work to be followed by the bank are as follows:-

1. Prevent failures from impacting business processes
2. Optimum server Utilization

3. Load balancing
4. Structural cabling.
5. Creating alternative fail over data centers
6. Creating fail over network infrastructure
7. Providing means of alternate access and authentication for users.
8. Moving important data to an alternate site.
9. Recovery of data at the alternate site.
10. Recovery of primary site and applications.
11. Down time reporting.

Data loss can occur for various reasons, including:-

a) Disk failures caused by hard ware failure, power outages or improper use.
b) Network problems leading to lost packets that are not acknowledged because of router congestion or other situations.
c) Virus infection, resulting in corrupted files
d) Flood, fire or any kind of natural catastrophic
e) Acts of terrorism

To counter these disasters with the minimum possible disruption to business operations and loss of valuable data, the system administrator and his assistant must constantly monitor the environment for threats to the assets of the organization. After these potential threats are identified, they must analysis whether the safe guards currently in place are sufficient, to mitigate the risk posed by the threats. If the safe guards are insufficient, the bank must consider implementing additional safeguards.

Disaster work disruption can happen due to the following factors and the recovery steps to be taken are mentioned against below:

A. Arising out of external factors.	
1.a. Disaster due to breakdown or fire	The possible causes of fire in and around the location must be analyzed in detail and all preventive measures required, for the protection of assets from fire accidents must be taken. One of the staff of the bank has been deputed to tackle the matter especially to report the top management level and also to fire rescue department of the Govt.
(b) Disaster due to floods/tsunami	In a flood/tsunami prone area, adequate care has to be taken for location of the building and for proper structural design to avoid damage due to flooding. To control the damage of data due to flood the data centre and DR centre should be located in two distant places.
(c) Disaster due to earthquake	Earthquake can cause considerable damage to assets, resulting in the loss of data. Adequate safety measures suggested by the local Government must be strictly adhered to. To control the damage of data due to flood the data centre and DR centre

	should be located in two distant places.
2. Disaster due to power failure	Suitable alternate arrangements to overcome the disaster due to power failure are to be kept ready. As a part of this generator has been installed in the bank. Further one of the staff member has been deputed to look after the same.
3. Disaster due to communication / connectivity failure	Redundancy measures must be made available and periodically checked to ensure that there is 'no interruption in connectivity. The person in charge of computer should report the matter to IT committee and IT committee may forwarded the same to the Board.
B.Arising out of data corruption/non-availability/unauthorized access of data	
1. Disaster due to lack of data access control mechanism	Proper logical access controls and user level privileges must be established and documented with due control mechanisms in Place.
2. Disaster due to lack of data consistency.	Direct modification/updating of data must be prevented. In case of exigency, such modification/updating of data must be done with proper authorizations only and must be documented. Logs must be made available.
3. Failure of regular data backup and verification of backup data periodically	Any disaster recovery plan can be effective only with a sound back up procedure adopted and meticulously followed by the institution.
4. Use of unauthorized Programs to access data	Authorized programs only must be used by branches/offices and they must be suitably protected from unauthorized access, alteration and misuse.
C. Arising out of failure of hardware and networking (LAN)	
1. Disaster due to breakdown of file server and damage to nodes and other hardware Peripherals, connectivity equipment, communication channels.	To obviate work disruption due to total damage to the filer server, nodes and other systems suitable backup measures are to be adopted.
2. Non-availability of hardware compatible with the available systems due obsolescence, mismatch specifications, etc.	Hardware requirements in the changing environment, at all levels, must be periodically reassessed and the required upgrades/add-on components/replacements must be taken up on need, taking cost into consideration.
3. Loss of connectivity/unauthorized connectivity in LAN environment	The LAN environment must be optimally utilized mplti-LAN and inter-LAN environment must be monitored properly with adequate security aspects.
D. Arising out of technology changes in software including operating system, application software, executable and packages	
I. Change in operating system, network operating system architecture due to upgrade/development.	Periodical upgrades/patches released by operating system/network operating system vendors must be procured and loaded into all the systems as a first-line security measure and such actions must be properly documented.
2. Lack of version control application packages/programs.	Any change effected in the application package or programs must be with a proper approval/ authorization only and due documentation. End users must be made aware of functional changes, if any.
3. Unsecured exposure of software to	All executable application programmed files must be secured

external environment	from exposure to external environment. Use of external programs to penetrate such executable must be totally curtailed. User rights must be properly defined on such executable file with access restrictions.
4. Lack of backup and library of programs/data	Proper backup and library of source codes and executable with compatible operating system versions must be maintained and recorded.
5. Non-availability inadequate documentation	Documentation for all application packages/programs must be prepared with due consideration for the end-user and their knowledge levels.
6. Corruption/collision/conflict of executable program files resulting in system hanging, denial of service.	Due care must be exercised when changing the programs/over-writing the executable. It must be ensured that whenever new executable are loaded, they are compatible with the earlier version and all the executable are compatible with a single version.
E. Arising out of human factors	
1. Lack of knowledgeable and trained professional.	Lack of knowledge must not be a reason for disaster. Adequate training has to be given to all personnel involved, to have a 'First and Second line' and to ensure business continuity and their knowledge must be refreshed periodically.
2. Sabotage created out of intentional or unintentional acts.	Access to the computer room/site must be strictly controlled. Proper vigilance measures must be in place to prevent network intrusions, hacking etc.
3. Disaster due to virus attacks.	All computer systems in use must be loaded with authorized 'Anti-Virus' software and must be kept operational always.
4. Instances relating to lack of physical access control, Piggy backing , social engineering, etc.	Prudence in handling human ware must be undertaken and staff integrity must be encouraged.
5. Other risk such as burglary, fraud, etc.	All safety and security measures required to safeguard the assets against a burglary and preventive measures to avoid commission of a fraud must be taken.

The aforesaid recovery measures come into action, after a disaster has occurred. During this phase, activities such as damage assessment and salvaging take place. Depending upon the impact of the disaster, critical activities are shifted to an alternate location or disaster recovery site which is kept ready always for resuming business activities at short notice.

software, comprising both the application software and system software, is vital to the operations of a computerized system. The system software comprising operating systems, compilers, utilities etc. have to be objectively procured to drive the software applications for meeting banking needs vendor policies and technological breakthrough result in development and availability of newer software directed at efficient utilization of the hardware. It changes the quality of banking products and methods of service delivery so the bank resolved to shift from TBA to networked online centralized banking solutions (CBS).