CLOUD4C

01 January 2022

BUSINESS CONTINUITY MANAGEMENT POLICY

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

Preparation

Draft	**Author**	**Date**
1.0	Sudheer G	16/04/2013
1.1	Sudheer G	14/03/2014
1.2	Soudha Rahman	01/06/2015
1.3	Deepthi Naidu	01/02/2016
1.4	Venkataniranjan.m	15/07/2016
1.5	M.Venkataniranjan	08/01/2017
1.5	M.Venkataniranjan	06/01/2018
1.6	M.Venkataniranjan	10/10/2018
1.6	M.Venkataniranjan	05/01/2019
1.6	M.Venkataniranjan	02/01/2020
1.6	M.Venkataniranjan	31/12/2020
1.6	M.Venkataniranjan	31/12/2021

Classification	**Storage Location**
Confidential	Shared folder

Review & Approval

Reviewer & Approver	**Version**	**Date**	**Reviewed Draft Version**
RS Prasad Rao	1.0	16/04/2013	1.0
RS Prasad Rao	1.1	14/03/2014	1.1
RS Prasad Rao	1.2	13/04/2015	1.2
RS Prasad Rao	1.3	01/02/2016	1.3
RS Prasad Rao	1.4	18/07/2016	1.4
RS Prasad Rao	1.5	16/01/2017	1.5
RS Prasad Rao	1.5	07/01/2018	1.6
RS Prasad Rao	1.6	10/10/2018	1.7
RS Prasad Rao	1.6	07/01/2019	1.7
RS Prasad Rao	1.6	03/01/2020	1.7
RS Prasad Rao	1.6	01/01/2021	1.7
RS Prasad Rao	1.6	01/01/2022	1.7

Release

FOR INTERNAL USE ONLY

Release Version	Date Released
1.0	16/04/2013
1.1	14/03/2014
1.2	13/04/2015
1.3	01/02/2016
1.4	18/07/2016
1.5	16/01/2017
1.5	07/01/2018
1.6	10/10/2018
1.6	07/01/2019
1.6	03/01/2020
1.6	01/01/2021
1.6	01/01/2022

Distribution List

Name	Designation	Department
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	Change Reason	Effective Date
1.1	Added statement of Confidentiality, Reviewed and no update	14/03/2014
1.2	Reviewed and updated IS aspects of business continuity	13/04/2015
1.3	Reviewed and no update	01/02/2016
1.4	Reviewed and updated version	18/07/2016
1.5	Reviewed and Updated version and scope	16/01/2017
1.5	Reviewed and no Update	07/01/2018
1.6	Reviewed and Updated training section 4.3 and section 4.5 Review of Business Continuity Plan	10/10/2018
1.6	No updates	05/01/2019
1.6	No updates	03/01/2020
1.6	No updates	31/12/2020
1.6	No updates	31/12/2021

STATEMENT OF CONFIDENTIALITY

© Copyright - Do Not Duplicate
FOR INTERNAL USE ONLY

This document contains proprietary trade secret and confidential information to be used solely for evaluating Cloud4C Services Private Ltd. The information contained herein is to be considered confidential. Customer, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by Cloud4C Services Private Ltd.

TABLE OF CONTENTS

FOR INTERNAL USE ONLY

1 INTRODUCTION

Business Continuity Management (BCM) is not just about disaster recovery, crisis management, risk management, or technology recovery. It is not a professional specialist discipline but a business owned and driven issue that unifies a broad spectrum of business and, management disciplines. In particular, it provides the strategic and operational framework to both review and where appropriate redesign the way Cloud4C provides its products and services whilst increasing its resilience to disruption, interruption or loss.

2 OBJECTIVE

The objective of this policy is to detail accountabilities, define planning standards and outline implementation requirements to minimize the effect of a disruption of services to Cloud4C and their customers, minimize financial losses and ensure a timely resumption of critical functions. In doing so, Cloud4C will more effectively protect the life and safety of its personnel, minimize the number of decisions which must be made following an emergency or business interruption, and decrease the organization's dependence on the participation of any specific person or group of people during the recovery. Cloud4C determines the requirements of information security and continuity of information security management in adverse situations i.e.; during a disaster.

3 SCOPE

This procedure shall apply to all employees of Cloud4C, its contractors, subcontractors, associated third parties who are users of Cloud4C services or who have access to Cloud4C facility. Cloud4C Services Private Limited is Sister concern company of CtrlS Data centres Ltd. The management and Support teams are the same. Hence the policy covers both Cloud4C.

4 POLICY STATEMENT

Cloud4C shall ensure that a formalized Business Continuity Program is developed which provides guidelines for development, maintenance, and exercising of Business Continuity Plans*.* More importantly, the policy seeks to provide for the resumption of time-sensitive business operations under pre-established timeframes, recovery of less time-sensitive business operations as required, restoration of the primary site and ultimately return to a permanent operating environment.

4.1 Business Continuity Plan

- A comprehensive Business Continuity Plan (BCP) shall be developed and implemented to maintain or restore business operations in the required time scales following an interruption to, or failure of, critical business processes. The BCP must include effective Disaster Recovery procedures for quickly recovering from an emergency with minimum impact to the company’s operations.
- Business Continuity Plan must be developed based on critical processes and related assets through identified through Business Impact Analysis.
- Business Impact Analysis must evaluate the impact of the interruptions in terms of damage scale and recovery period. Business Impact Analysis also includes identification of risk and threats affecting Cloud4C which enables the formulation of the Business Continuity Plan.

© **Copyright - Do Not Duplicate**

FOR INTERNAL USE ONLY

4.2 Testing of Business Continuity Plan

- BCP must be tested at least once in a year to identify incorrect assumptions, oversights, or changes in equipment or personnel.
- Test results should be used to revise the BCP.
- The test results should be reported to senior management.

4.3 Training

Cloud4C shall ensure all team members undergo periodical training and are apprised of the requirements outlined in this procedure.

4.4 Business Continuity Management Process

Processes shall be put in place as per the tested and approved BCP to ensure the required Level of continuity for information security during an adverse situation, prompt resumption of business processes in the event of a business interruption via detailed plans and processes that form part of their Business Continuity Plan (BCP).

4.5 Review of Business Continuity Plan

- BCP must be regularly reviewed and updated on an annual basis to ensure that the BCP considers the effectiveness of information security continuity controls, the current nature of business processes, infrastructure, personnel, etc.
- Management Review Committee shall review suitability and adequacy of the Business Continuity Management Policy document during management review meetings

5 COMPLIANCE WITH THE POLICY

Compliance with the Business Continuity Management Policy and Procedure shall be mandatory. Head – Information Security, assisted by Information Security Forum shall ensure continuous compliance with this policy and procedure within Cloud4C. The periodic review shall be conducted by Departmental Heads and shall be reported to Head – Information Security to verify compliance with this policy and procedure. All employees shall be responsible to inform the Head – Information Security if any policy breach is discovered or identified.

6 VIOLATION WITH THE POLICY

Any user found to have violated this Business Continuity Management Policy and Procedure may be subjected to disciplinary action, up to and including termination of employment.

6.1 Consequences of violation of the Policy

Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets, and
- Other actions as deemed appropriate by Management, Human Resources, and the Legal Department.

7 CONTACT ROLE FOR CLARIFICATION REGARDING THE POLICY

© Copyright - Do Not Duplicate

FOR INTERNAL USE ONLY

The sponsor of this policy is the Head – Information Security. Head – Information Security shall be responsible for the maintenance and accuracy of the policy. Any questions regarding this policy shall be directed to the Head – Information Security.

8 WAIVER CRITERIA

This Policy and Procedure is intended to address information security requirements. Requested waivers shall be formally submitted to the Head – Information Security including justification and benefits attributed to the waiver for approval. The waiver shall only be used in exceptional situations for communicating non-compliance with the policy for a specific period (subject to a maximum period of 30 days). After the period, the need for the waiver shall be reassessed and re-approved, if necessary. The waiver shall not be provided for more than three consecutive terms. The waiver shall be monitored to help ensure its concurrence with the specified period and exception.

© Copyright - Do Not Duplicate

FOR INTERNAL USE ONLY