CLARISYNC

TRUST CENTRE

Business Continuity & Disaster Recovery Summary

TRUST CENTRE

Business Continuity & Disaster Recovery Summary

01

Introduction

Clarisync recognizes the importance of maintaining service availability and protecting customer data against unexpected disruptions.

Our Business Continuity and Disaster Recovery (BCDR) approach is designed to support the continued delivery of our services, minimize operational disruption and enable the recovery of systems and data following an interruption.

This document provides an overview of the practices and arrangements supporting the continuity and recovery of the Clarisync platform.

02

Business Continuity Approach

Business continuity is supported through a combination of infrastructure management, operational procedures, data protection measures and recovery arrangements.

- Maintaining the availability of critical platform services.
- Protecting customer information against accidental loss or corruption.
- Reducing the impact of infrastructure and application disruptions.
- Establishing recovery procedures for affected systems.
- Coordinating technical and operational teams during service interruptions.
- Reviewing recovery arrangements to identify opportunities for improvement.

03

Infrastructure Resilience

Clarisync platform architecture and services selected for each customer environment support the operation, management and recovery of the platform.

- Dedicated cloud infrastructure environments for individual customers, where configured.
- Managed cloud services supporting application and database operations.
- Controlled network architecture and infrastructure configurations.
- Infrastructure health and performance monitoring.
- Controlled deployment and configuration management.
- Centralized visibility into relevant infrastructure events.

The specific resilience capabilities available to a customer depend on the architecture,region, service configuration and contracted service scope.

04

Data Backup and Protection

Data protection is an important part of Clarisync's continuity strategy. Backup and recovery arrangements are used to support the restoration of relevant information following accidental deletion, corruption or infrastructure disruption.

4.1 Automated Backups

Automated backup mechanisms are used to protect relevant application and database information. Backup coverage and frequency depend on the applicable infrastructure and service configuration.

4.2 Data Versioning

Versioning capabilities may be used for supported data and objects to maintain recoverable versions and help address unintended modification or deletion.

4.3 Backup Protection

Access to backup resources is controlled to reduce the risk of unauthorized access, modification or deletion.

4.4 Data Recovery

Recovery procedures support the restoration of relevant data from available backups and recovery points when required. Restored data and services are subject to appropriate validation before being returned to normal use.

Backup frequency, retention periods, coverage and restoration capabilities may vary by environment and are governed by the relevant technical configuration and service arrangements.

05

Disaster Recovery

Disaster recovery arrangements are designed to restore affected services following significant infrastructure failures, application disruptions or other events that impact normal operations.

The recovery process generally involves:

Incident Identification	Identifying the disruption and assessing its impact on affected services.
Impact Assessment	Determining the affected infrastructure, applications, databases and customer environments.
Recovery Activation	Engaging relevant technical and operational personnel and initiating appropriate recovery procedures.
System Restoration	Restoring affected infrastructure, application services and data using available recovery mechanisms.
Validation	Verifying system functionality, data integrity and service operation before returning to normal service.
Post-Recovery Review	Documenting the incident, identifying contributing factors and evaluating opportunities for improvement.

06

Recovery Objectives

Clarisync uses recovery objectives to guide the restoration of services and the protection of customer data. Two common measures are considered:

6.1 Recovery Time Objective (RTO)

The Recovery Time Objective is the target period within which affected services should be restored following a disruption.

6.2 Recovery Point Objective (RPO)

The Recovery Point Objective is the maximum targeted period of data loss measured in time, based on the most recent recoverable data point.

Actual recovery objectives depend on the service configuration, infrastructure architecture, nature and severity of the disruption, and applicable customer commitments. Specific RTO and RPO targets should be established and communicated through the relevant service agreement or customer-specific documentation.

> Unless expressly agreed in writing, this summary does not establish a guaranteed RTO or RPO for any particular customer environment.

07

Monitoring and Operational Readiness

Clarisync uses infrastructure and application monitoring to maintain visibility into system health and identify potential service disruptions.

- Infrastructure and application health monitoring.
- Database and server performance visibility.
- Identification of abnormal system behaviour.
- Monitoring of relevant service and infrastructure events.
- Investigation and escalation of operational issues.

These capabilities help technical teams identify potential problems and take appropriate corrective action.

08

Business Continuity and Incident Coordination

During a significant service disruption, Clarisync coordinates relevant technical and operational teams to manage the situation.

The response focuses on:

- Assessing the impact on customer-facing services.
- Prioritizing recovery activities.
- Coordinating infrastructure, engineering and support resources.
- Keeping relevant stakeholders informed in accordance with applicable arrangements.
- Validating service restoration.
- Recording the incident and associated corrective actions.

Customer communications are managed in accordance with applicable service agreements and support arrangements.

09

Testing and Continuous Improvement

Business continuity and disaster recovery arrangements are subject to review to maintain their relevance and effectiveness.

Review activities may include:

- Reviewing backup and recovery configurations.
- Assessing infrastructure resilience.
- Reviewing recovery procedures.
- Evaluating operational incident records.
- Identifying improvements to recovery processes.
- Reviewing relevant technical and operational documentation.

Recovery testing activities and their results should be documented where performed, and identified improvement actions should be addressed through the appropriate internal processes.

The frequency and scope of recovery testing depend on the applicable systems, operational priorities and established internal plans.

10

Roles and Responsibilities

Effective continuity and recovery require coordination across the teams responsible for operating and supporting the Clarisync platform.

AREA	GENERAL RESPONSIBILITY
Engineering and Infrastructure	Assess technical impact, investigate infrastructure or application issues, and perform approved restoration activities.
Operations and Support	Coordinate incident handling, track service impact and manage customer communications through established channels.
Customer	Maintain appropriate user and data management practices, provide relevant information during investigations and follow customer-side continuity procedures where applicable.

Specific responsibilities may be further defined in applicable service agreements, support procedures and customer-specific operating arrangements.

11

Customer Considerations

Customers should consider their own business continuity requirements when using the Clarisync platform. In particular, Customers should:

- Maintain appropriate internal procedures for business activities that depend on the platform.
- Ensure that authorized users and relevant support contacts are kept up to date.
- Retain copies of information where required by their own business or regulatory obligations.
- Understand any customer-specific backup, export, recovery and service commitments agreed with Clarisync.
- Notify Clarisync promptly when a suspected service issue materially affects their use of the platform.

12

Contact Information

For questions regarding business continuity, disaster recovery or service resilience, please contact the Clarisync team.