Policy Type: Business Continuity & Disaster Recovery Policy **Policy Number: BCD.1.0.0**

Business Area: Information Technology

Policy Owners: CTO
Sr. Director of Engineering/Director of Operations
Security and Operations Engineer

Effective Date: 1/1/2019

Purpose

The purpose of this business continuity plan is to prepare Cloudnosys in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Scope

All Cloudnosys IT systems that are business critical and/or process, store, or transmit confidential information. This Policy applies to all employees of Cloudnosys and to all external parties, including but not limited to Cloudnosys consultants, contractors, business partners, vendors, suppliers, outsource service providers, and other third-party entities with access to Cloudnosys IT networks and system resources.

Roles and Responsibilities

Role	Responsibility
Emergency Response Team Manager / CTO	The person who deems and declares an incident to be an emergency and is responsible for the management of emergency operations for the duration of the event. He/she will set the incident objectives, strategies, and priorities and has overall responsibility during the incident or event. In the event the CTO is unavailable, consult the organization chart for the next responsible person.
Departmental Continuity Leader	The person responsible for the management of emergency operations specific to his/her department. He/she will set the incident objectives, strategies, and priorities and has overall responsibility within his/her division during the incident or event. He/she is generally the Department VP, and reports activities to the Emergency Response Team Manager during the event. He/she will have oversight overall tactical operations that are carried out by his/her department. Example departments include: Engineering, Revenue, Finance and People Resources

Copyright © 2019 Cloudnosys. All Rights Reserved.

Director / Manager	The person responsible for conducting tactical operations to carry out the plan in each division. He/she develops the tactical objectives and organization, and directs all tactical
	resources for the division. Will serve as backup to the Departmental Continuity Leader for the division during the event.
Public Information Officer	The person responsible for serving as the conduit for information to internal and external stakeholders, including the media or other organizations seeking information directly from the incident or event. Ownership will be managed by the Chief Marketing Officer with direct support from the Customer Success team.
Emergency Response Team Management Committee	The committees comprised of Facility Leaders & Department Leaders who are responsible for documenting all emergency response activities occurring at each facility throughout the company. The notes/documentation may become critical for insurance reporting purposes. This committee will also be responsible for keeping employee lists and contact information current to within 3 months, in the event personnel need to be reached during an emergency event. This responsibility is owned by the People team with support from the Operations Team.

Policy 1. Information Security Continuity

a. Planning information security continuity

The possibility of a major event is real and requires contingency planning; therefore, Cloudnosys has developed a business continuity plan. This plan will provide guidance to continuing daily activities in the event of a major disruption to Cloudnosys's business. It is the goal of Cloudnosys to first and foremost ensure employee health and safety during an emergency event.

The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the business.

Cloudnosys production systems are classified as Category I, comprising those functions whose loss could cause a major impact to the business within 2 hours.

Systems supporting critical business functions are classified as Category II - requiring processing support within 48 hours of an outage.

System assessment and classification will be repeated on a regular basis to ensure that changes to our processing and environment are reflected in recovery planning.

Cloudnosys recognizes the low probability of severe damage to its online platform. Nevertheless, because of the potential impact to the Cloudnosys platform, a plan for reducing the risk of damage from a disaster, however unlikely is vital. The Cloudnosys Business Continuity Plan is designed to reduce the risk to an acceptable level by ensuring the restoration of Critical processing within 24 hours, and all essential production (Category II processing) within 2 week(s) of the outage.

Copyright © 2019 Cloudnosys. All Rights Reserved.

The Plan identifies the critical functions of the Cloudnosys platform and the resources required to support it. The Plan provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response and that the proper steps will be carried out to permit the timely restoration of services.

This Business Continuity Plan is distinct from the Information Security Incident Response Plan, which provides guidance on response procedures in the event of an information security breach or failure that threatens Cloudnosys's data or systems.

In the case of an information security event, refer to the Information Security Incident Response Plan.

b. Implementing information security continuity

Disaster Response

This section describes six required responses to a disaster, or to a problem that could evolve into a disaster:

1. Detect and determine a disaster condition
2. Notify persons responsible for recovery
3. Initiate the Business Continuity Plan
4. Activate teleworking and the failover site
5. Disseminate Public Information
6. Provide support services to aid recovery

1. Disaster Detection and Determination

The detection of an event which could result in a disaster affecting Cloudnosys's online platform or their ability to support the platform, is the responsibility of whom first discovers or receives information about an emergency situation developing.

2. Disaster Notification

The reporting individual will follow the existing procedures and notify the Emergency Response Team Manager.

3. Plan Activation

Once the Emergency Response Team Manager has declared an emergency, the following must be notified:

- CEO
- CTO
- VP – Customer Success
- Sr Director of Engineering/Director of Operations
- Boulder Office

In the state of emergency reporting structures will be modified in the following ways:

The Public Information Officer will no longer report to his/her direct supervisor but rather directly to the Emergency Response Team Manager.

Copyright © 2019 Cloudnosys. All Rights Reserved.

The Emergency Response Team Manager will be responsible for contacting all Emergency Response Team Committee Members, Departmental Continuity Leaders, and activating the declared emergency.

The Departmental Continuity Leaders will assume the role of Manager for his/her department and report directly to the Emergency Response Team Manager. He/she will provide support for the Emergency Response Team by coordinating resources, administrative duties, and additional services needed by the team. He/she will communicate with the Emergency Response Team Manager directly.

4. Activation of Teleworking and Designated Failover Site

The responsibility for activating any of the designated hot sites or back-up resources is delegated to the Chief Technology Officer. In the absence of the CTO, responsibility reverts to the Sr. Director of Engineering/Director of Operations. Within 2 hours of the occurrence, the CTO, or alternate, determines the prognosis for recovery of the damaged functional area through consultation with the designed functional area (Security Team, Office Management Team, etc)

In the event that the Cloudnosys Corporate office is not available, users shall work remotely from a safe location of their choosing. Users shall utilize electronic and telephonic communications to communicate their status and availability to work.

The Emergency Response Team shall first review the availability of AWS regions and services and make a determination as to which region shall be used to restore operations. Rebuilding the Cloudnosys production environment shall be the primary goal of the Emergency Response Team and available engineering staff once team members have established team communications and safe working environments.

Information Security Continuity

Cloudnosys shall implement the same production security controls currently in use when it rebuilds the production environment.

5. Dissemination of Public Information

The Public Information Officer is responsible for directing all meetings and discussions with the news media and the public, and in conjunction with Cloudnosys personnel not actively participating in the recovery operation. In the absence of the Public Information Officer, the responsibility reverts to the senior official present at the scene.

6. Disaster Recovery Strategy

The disaster recovery strategy explained below pertains specifically to a disaster disabling the main Cloudnosys production platform or the Corporate Office. This section addresses three phases of disaster recovery:

- Emergency
- Backup
- Recovery

Copyright © 2019 Cloudnosys. All Rights Reserved.

EMERGENCY PHASE

If the emergency situation appears to affect the service, either through damage to data processing or support facilities, the Departmental Continuity Leader for Operations will closely monitor the event, notifying Emergency Response Team Manager as required to assist in damage assessment.

The Emergency Response Team Committee and Emergency Response Team Manager remains active until recovery is complete to ensure that the platform will be ready in the event the situation changes.

BACK-UP PHASE

In the initial stage of the back-up phase, the goal is to resume processing critical applications. Processing will resume either at the main availability zone or in case that fails then on an alternative zone. In case of full GCP region failure we will depend on GCP recovery procedures of that region to be able to restore systems.

In the back-up phase, the alternative availability zone will be used to run critical applications (Category I). During this period, processing of these systems resumes, possibly in a degraded mode, up to the capacity of the alternate zone till the main zone returns to full operational status if possible.

RECOVERY PHASE

The time required for recovery of the functional area and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several hours to several days. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated availability zone. The primary goal is to restore normal operations as soon as possible.

c. Verify, review and evaluate information security continuity

BC PLAN MAINTENANCE

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the updated Plan; and training personnel. The Emergency Response Team Management Committee are responsible for this comprehensive maintenance task.

BC PLAN TESTING

Testing the Business Continuity Plan is an essential element of preparedness. Partial tests of individual components and recovery plans of specific business areas will be carried out on a regular basis. A comprehensive exercise of our continuity capabilities and support by our designated recovery facilities will be performed on an annual basis.

Copyright © 2019 Cloudnosys. All Rights Reserved.