Disaster Recovery Policy

Beyond

March 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.2, A1.3

Table 2: Document history

Date	Comment
Aug 14 2023	Initial document
Jan 25 2024	Updated staff
Mar 11 2024	Updated staff

1 Purpose and Scope

a. The purpose of this policy is to define the organization's procedures to recover Information Technology (IT) infrastructure and IT services within set deadlines in the case of a disaster or other disruptive incident. The objective of this plan is to complete the recovery of IT infrastructure and IT services within a set Recovery Time Objective (RTO).

b. This policy includes all resources and processes necessary for service and data recovery, and covers all information security aspects of business continuity management.

c. This policy applies to all management, employees and suppliers that are involved in the recovery of IT infrastructure and services within the organization. This policy must be made readily available to all whom it applies to.

2 Background

a. This policy defines the overall disaster recovery strategy for the organization. The strategy describes the organization's Recovery Time Objective (RTO), which is defined as the duration of time and service level for critical business processes to be restored after a disaster or other disruptive event, as well as the procedures, responsibility and technical guidance required to meet the RTO. This policy also lists the contact information for personnel and service providers that may be needed during a disaster recovery event.

b. The following conditions must be met for this plan to be viable:

    i. All equipment, software and data (or their backups/failovers) are available in some manner.

    ii. If an incident takes place at the organization's physical location, all resources involved in recovery efforts are able to be transferred to an alternate work site (such as their home office) to complete their duties.

    iii. The Information Security Officer is responsible for coordinating and conducting an annual review of this continuity plan.

c. This plan does not cover the following types of incidents:

    i. Incidents that affect customers or partners but have no effect on the organization's systems; in this case, the customer must employ their own continuity processes to make sure that they can continue to interact with the organization and its systems.

    ii. Incidents that affect cloud infrastructure suppliers at the core infrastructure level, including but not limited to Google and Amazon Web

Services. The organization depends on such suppliers to employ their own continuity processes.

3 Policy

a. *Remote Work Continuity*

   i. In the event of the organization's primary digital infrastructure becoming unavailable, an alternate digital platform or set of tools shall be utilized by designated personnel. The organization's primary and alternate digital work environment will include Google Workspace, Salesforce, Slack, Zoom, Tettra, 1password, Ramp, Rippling, Docusign, Outlaw, Netsuite, Jira, and Google Cloud Platform

   ii. All employees are required to ensure continuity of work and maintain operations during any such digital disruption. Additionally, all employees are expected to be adaptable to transitioning to the designated alternate digital platforms to ensure seamless work continuation.

b. The organization's Recovery Time Objective (RTO) is 24 hours. Relocation and restoration of critical services and technologies must be completed within this time period.

c. *Notification of Plan Initiation*

   i. The following personnel must be notified when this plan is initiated:

   1. Julie Brinkman, CEO
   2. David Kelso, CTO, DPO
   3. Lindsey Branding, General Counsel
   4. Ricardo Marques, Platform Staff Engineer
   5. Paula Justi, Director of Platform Engineering
   6. All other Beyond employees, through email if available

   i. Francois Toubol, VPE, is responsible for notifying the personnel listed above.

d. *Plan Deactivation*

   i. This plan must only be deactivated by Julie Brinkman, CEO.

   ii. In order for this plan to be deactivated, all relocation activities and critical service / technology tasks as detailed above must be fully completed and/or restored. If the organization is still operating in an impaired scenario, the plan may still be kept active at the discretion of Julie Brinkman, CEO.

   iii. The following personnel must be notified when this plan is deactivated:

   1. Julie Brinkman, CEO
   2. David Kelso, CTO, DPO

    3. Lindsey Branding, General Counsel
    4. Ricardo Marques, Platform Staff Engineer
    5. Paula Justi, Director of Platform Engineering
    6. All other Beyond employees, through email if available

e. The organization must endeavor to restore its normal level of business operations as soon as possible.