Disaster Recovery Policy

Sour Lemon Digital, LLC

May 2023

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.2, A1.3

Table 2: Document history

Date	Comment
Nov 1 2022	Initial document
May 15 2023	Adding critical systems appendix

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 eventual physical location, all resources involved in recovery efforts will be able to be transferred to an alternate work site (such as their home office) to complete their duties.

    iii. The CIO is responsible for coordinating and conducting a bi-annual (at least) rehearsal 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, Heroku, and

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

3 Policy

a. *Relocation*

   i. If the organization's eventual primary work site is unavailable, an alternate work site shall be used by designated personnel. The organization's alternate work site for approved personnel will be virtual/home office.

   ii. The personnel required to report to the alternate work site during a disaster includes [Brian Racer, CIO and Tony Vanden Bush, CEO].

b. *Critical Services, Key Tasks and, Service Level Agreements (SLAs)*

   i. The following services and technologies are considered to be critical for business operations, and must immediately be restored (in priority order):

      1. AWS Services and Infrastructure
      2. Cloudflare Web Application Firewall

c. The organization's Recovery Time Objective (RTO) is 3 days. Relocation and restoration of critical services and technologies must be completed within this time period.

d. *Notification of Plan Initiation*

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

   1. Tony Vanden Bush, CEO
   2. Brian Racer, CIO

e. *Plan Deactivation*

   i. This plan must only be deactivated by the CIO.

   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 [person or persons with authority to deactivate the plan, including job title].

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

      1. CEO

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

g. A list of relevant points of contact both internal and external to the organization is enclosed in Appendix A.

h. During a crisis, it is vital for certain recovery tasks to be performed right away. The following actions are pre-authorized in the event of a disaster recovery event:

    i. CIO must take all steps specified in this disaster recovery plan in order to recover the organization's information technology infrastructure and services.

    ii. CIO is authorized to make urgent purchases of equipment and services up to $2,000.

    iii. CEO is authorized to communicate with clients.

    iv. CEO is authorized to communicate with the public.

    v. CEO is authorized to communicate with public authorities such as state and local governments and law enforcement.

i. Specific recovery steps for information systems infrastructure and services are provided in Appendix B.

4 Appendix A: Relevant Points of Contact

Internal Contacts

Name	Job Title	Phone Number	Email Address	Alternate Contact
Tony Vanden Bush	CEO		tony@monicur.com	
Brian Racer	CIO	720-722-3769	brian@monicur.com	

5 Appendix B: Recovery Steps for Information Systems Infrastructure & Services

Specific recovery procedures are described in detail below:

System to be recovered	Person Responsible	Person(s) Notified When Complete
AWS	CIO	CEO
Cloudflare	CIO	CEO