Disaster Recovery Policy

Discotheque Inc

November 2020

Contents

1 Background **2**

2 Policy **3**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	A1.2, A1.3

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

#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.

1 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 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.

2 Policy

a. *Relocation*

   i. If the organization's primary work site is unavailable, an alternate work site shall be used by designated personnel. The organization's alternate work site: Remote work provided by each employee.

   ii. The personnel required to report to the alternate work site during a disaster includes Chief Technology Officer and the Engineering Team.

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. Slack and Microsoft Teams APIs.

      2. JustDisco Dashboard

c. Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

Meeting response times associated with service-related incidents.

Recovery Time Objective (RTO) $<$ 45 min

The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

Recovery Point Objective (RPO) $<$ 30 min

The interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or "tolerance."

Appropriate notification to Customer for all scheduled maintenance.

a. Service Assumptions

Assumptions related to in-scope services and/or components include:

Changes to services will be communicated and documented to all stakeholders. Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

a. Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

Telephone support : 9:00 A.M. to 8:00 P.M. EST Monday – Friday Calls received out of office hours will be forwarded to a mobile phone and best efforts will be made to answer / action the call, however, there will be a backup answerphone service

Email support: Monitored 9:00 A.M. to 8:00 P.M. EST Monday – Friday Emails received outside of office hours will be collected, however, no action can be guaranteed until the next working day

a. Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service-related incidents and/or requests submitted by the Customer within the following time frames:

0-8 hours (during business hours) for issues classified as High priority. Within 48 hours for issues classified as Medium priority. Within 5 working days for issues classified as Low priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

a. *Notification of Plan Initiation*

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

    1. Chief Executive Officer, Chief Operating Officer

    i. Joseph Estrada, CTO is responsible for notifying the personnel listed above.

b. *Plan Deactivation*

    i. This plan must only be deactivated by the Chief Technology Officer, Chief Executive Officer or the Chief Operating Officer.

    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 the Chief Executive Officer or the Chief Operating Officer.

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

        1. Chief Executive Officer, Chief Operating Officer

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

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

e. 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. Chief Technology Officer must take all steps specified in this disaster recovery plan in order to recover the organization's information technology infrastructure and services.

    ii. Chief Technology Officer is authorized to make urgent purchases of equipment and services up to [amount].

    iii. Chief Technology Officer is authorized to communicate with clients.

    iv. Chief Technology Officer is authorized to communicate with the public.

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

    vi. Chief Technology Officer is authorized to cooperate with Amazon Web Services and other suppliers.