

Disaster Recovery Policy

ACME Evil Anvil Corporation

January 2019

Contents

| | | |
|----------|---|----------|
| 1 | Background | 2 |
| 2 | Policy | 3 |
| 3 | Appendix A: Relevant Points of Contact | 5 |
| 4 | Appendix B: Recovery Steps for Information Systems Infrastructure & Services | 6 |

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 is located at [list the address of the alternate work site that the organization will use].
- ii. The personnel required to report to the alternate work site during a disaster includes [list the personnel titles responsible for reporting to the alternate work site].

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. [list the critical services and technologies that must remain running during a disaster]
- ii. The following key tasks and SLAs must be considered during a disaster recovery event, in accordance with the organization's objectives, agreements, and legal, contractual or regulatory obligations:
 1. [list of key tasks / SLAs that must be kept operational, with respective deadlines]

c. The organization's Recovery Time Objective (RTO) is [set the maximum amount of time before critical processes must be restored, to include relocation and getting critical services/technologies back online]. 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. [list all personnel (including titles) that must be notified of plan initiation]
- i. [person responsible for notifications, including title] is responsible for notifying the personnel listed above.

e. *Plan Deactivation*

- i. This plan must only be deactivated by [person or persons with authority to deactivate the plan, including job title].
- 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. [list all personnel (including titles) that must be notified of plan activation]
- 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. [job title] must take all steps specified in this disaster recovery plan in order to recover the organization's information technology infrastructure and services.
 - ii. [job title] is authorized to make urgent purchases of equipment and services up to [amount].
 - iii. [job title] is authorized to communicate with clients.
 - iv. [job title] is authorized to communicate with the public.
 - v. [job title] is authorized to communicate with public authorities such as state and local governments and law enforcement.
 - vi. [job title] is authorized to cooperate with [name of supplier/outsourcing partner].
 - vii. [add/modify/remove authorizations in this section as necessary]
- i. Specific recovery steps for information systems infrastructure and services are provided in Appendix B.

3 Appendix A: Relevant Points of Contact

Internal Contacts

| Name | Job Title | Phone Number | Email Address | Alternate Contact |
|------|-----------|-----------------|------------------|----------------------|
|------|-----------|-----------------|------------------|----------------------|

External Contacts

| Name | Job Title | Phone Number | Email Address | Alternate Contact |
|------|-----------|-----------------|------------------|----------------------|
|------|-----------|-----------------|------------------|----------------------|

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

Specific recovery procedures are described in detail below:

| Recovery Procedure | Person Responsible | Person(s) Notified When Complete |
|-------------------------|--------------------|----------------------------------|
| System to be recovered: | | |
| task 1: | | |
| task 2: | | |
| System to be recovered: | | |
| task 1: | | |
| task 2: | | |