

June 2024

Disaster Recovery Procedure | Procedure

PROCEDURE OWNER: Technology Department

PROCEDURE APPROVED BY: Director of Technology, kbridges@water.org

PROCEDURE CONTACT: Technology Department, help@water.org

Procedure Contents

- I. [Procedure Overview](#)
- II. [Procedure, Approvals, and Responsibilities](#)
- III. [Additional Resources](#)

I. Procedure Overview

Purpose of Procedure

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for critical technology platforms. This document summarizes our recommended procedures. In an emergency, modifications to this document may be made to ensure the physical safety of our people, systems, and data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

II. Procedure, Approvals, and Responsibilities

The purpose of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations.

We have taken a cloud-based approach to mitigate risk to the organization, while providing business continuity, security enhancements, and enterprise class of service. We have sought out the best services in each vertical that is also conducive to the budgetary requirements.

2.1 Backup Strategy

There are key business processes and agreed backup strategies provided by each service/system. The strategy chosen is for all business systems to be in a decentralized and separate hosting environment. Each separate environment is covered by a unique Service Level Agreement (SLA) by the company providing the services. Please refer to our Backup and Restoration Procedure regarding the strategy for Microsoft and Office backups. For all remaining systems, please reach out to the Technology Department (help@water.org) or the Business Lead identified for each system for more details.

2.2 Risk Management

Due to the inherent lack of risk by using separate systems hosted by the vendors and solution providers, most risks are mitigated. Breaches are still a possibility due to social engineering and human error. Please refer to our Security Incident Handling Policy and Procedure for more details.

2.3 Activation of Emergency Response Team

When a major incident occurs the Technology Team must be activated. The Technology Team will then decide the extent to which the systems are affected and what if any action can be done by Water.org staff. If the incident is major, it might require notification to the entire staff. This decision will go from the Technology Team to the Leadership Team, and All correspondence will be approved, as necessary.

- Initial notification/alert should be emailed to help@water.org
- If request is not immediately addressed and appropriate calls to the respective people in this order:
 - Kevin Bridges +1 816 674 6294
 - James Boomer +1 816 674 5355
 - Jennifer Riddle +1 816 301 5131
 - Atman Walters +1 816 898 3594

2.4 Corporate Insurance

As part of the company's disaster recovery and business continuity strategies an insurance policy has been put in place. Please refer to the corporate insurance policy managed by the Finance and HR teams for more details.

2.5 Disaster Recovery Plan Exercising

Disaster recovery plan (DRP) exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

2.6 Legal Action

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be.

The company legal department and Crisis Management Team (CMT) will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

Governance

The **Technology Department** is the owner of this procedure and is responsible for reviewing, implementing, amending, and making recommendations for updates or changes to these procedures in alignment with the business needs of Water.org.

III.Additional Resources

Contact for Support

Technology Department, help@water.org

Related Policies

Disaster Recovery Plan
Security Incident Handling Policy and Procedure
Backup and Restoration Procedure
Corporate Insurance Policy

