

DISASTER RECOVERY PLAN

**United Systems Access, Inc.
United Systems Access Telecom, Inc.**

DISASTER RECOVERY PLAN

I. Overview

The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples any of the various phone service-related computer systems operated by United Systems Access, Inc. and United Systems Access Telecom, Inc. (USA).

II. Description and Location of Systems

USA has four types of systems in its computer network:

1. Systems visible to the customer, such as our website and e-mail system;
2. Systems used to support these systems, such as database servers;
3. Systems used internally for operations and computer support, such as billing software and systems; and
4. Individual desktop and laptop systems.

The servers in types 1 and 2 are located in a secure, yet highly accessible facility in Waltham, Massachusetts. Other systems are distributed across our network, including facilities in Waltham, Massachusetts; Woburn, Massachusetts; Kennebunk, Maine; and Portland, Maine.

III. Normal Systems Operation and Disaster Prevention

All of the servers are backed up daily, and the backup tapes are removed from the premises. Data from desktop PCs is stored on central servers that are also backed up every day. Monthly backups of critical systems are archived. This helps to both prevent loss of data resulting from a disaster and provides a systems for recovery of the data. In the event of a systems failure, these backups can be used to quickly restore any and all systems. In addition, the availability of multiple facilities allows us to bring our systems back online even if an entire site becomes unavailable. We are also currently building out these facilities to house hot-spare servers to further reduce systems-related downtime to hours rather than days.

IV. Initiation of Disaster Recovery

Upon knowledge that a disaster has occurred, everyone on the Disaster Recovery List (DRL) will be notified by telephone or pager. The plan, along with the DRL and contact numbers, is posted at each of the offices mentioned above. The Disaster Recovery Team (DRT) is comprised of the following people:

Steve Gilbert – President / Team Manager
Phil Freed – IT
Laura Gibisser – IT
Tom Bergeron – Operations Manager / Public Relations

The DRT oversees the entire recovery process. The DRT Manager has the final authority on decisions that must be made during the recovery.

A Recovery Control Center (RCC) will be established for the DRT to coordinate the recovery process. All information should emanate from and be relayed to the RCC. However, newspapers, radio, TV reporters or members of the general public may want information about the company and the emergency situation – all team members and USA personnel are required to pass along requests for information to the Public Relations contact. The Public Relations contact is the only person authorized to make statements to the media.

V. Systems Analysis and Course of Action

A systems analysis will be performed to determine the exact systems that are down. This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. With respect to the facility, evaluation of damage to the structure, electrical system, air conditioning, and building network should be conducted. If estimates from this process indicate that recovery at the original site will require more than 5 days, migration to another site is recommended.

The primary goal is to determine where the recovery should take place and what hardware must be ordered immediately. The DRT will then formulate a course of action. Each member of the DRT will be charged with his or her responsibilities in order to carry out the plan and will report progress to the Team Manager as often as necessary. Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

Throughout disaster recovery, the Team Manager will keep an Operations Log, an official record of all activities conducted by the DRT. The Team Manager, will at the very least, record the following information in the Log:

1. The date and time that the recovery process begins and ends operations
2. Who is on the DRT and any individual involved in the recovery process
3. All critical information provided to the DRT, including, but not limited to: systems affected, contacts with personnel and general public, TV and radio press conferences or announcements, copies of press releases or proclamations, pertinent newspaper stories related to the events of the disaster and/or to USA in particular, internal reports to or from the DRT

V. Post-Recovery

Once all systems are operational, the Team Manager will prepare a report on the events that led up to the disaster, causes of downtime, and recommendations for improvement of system protection. In addition, the report will help maintain this disaster recovery plan and should suggest additional procedures.