

### Definition

A disaster is any event that causes the computer systems to be unavailable to supply correct services to users. Disaster recovery is a plan which is developed to protect the computing environment, to re-establish computer and network operations, and to identify and address the critical application needs of the institution in case of disaster.

### Standards

There are no current standards for disaster recovery procedures.

### Best Practices

#### General Framework

In order to have an effective disaster recovery plan, an organization must:

- Develop a framework for disaster recovery policy, procedures and standards.
- Define a framework for procedures to interface between related groups in case of a disaster.

#### Recovery Plan

To have an effective disaster recovery plan, you must develop an organization responsible for writing and maintaining it. The people in this organization must, in turn, develop the plan, and identify who has a role to play in case of information or network disaster. These tasks are carried out as follows:

- Develop disaster recovery guidelines for each corporate application, including items such as:
  - Employee roles and responsibilities.
  - Recovery team roles and responsibilities.
  - Recovery priority for each application.
  - Operational guidelines.
  - Location of production software and data.
  - Location of offsite / onsite backup systems and data.
  - Arrangements with backup and recovery vendors based on costs, capabilities and required response time.
  - Communication trees including names, roles and responsibilities, regular and alternate phone and fax numbers and addresses.
  - Procedures to maintain the communication trees.
  - Maximum waiting times.
  - Provision to relocate key staff and recovery teams after a disaster.
- Assess the effectiveness of existing inventory tracking procedures for computer hardware, network equipment, software packages and data storage media.
- Assess the cost-effectiveness of alternative backup and recovery solutions. Alternatives could include: in-house storage, reciprocal agreements, hot site vs. cold site options, etc.
- Recommend Solutions
- Negotiate backup and recovery arrangements with vendors if necessary.

#### Technical Procedures

Technical procedures should cover the following tasks:

- Develop and maintain a detailed up-to-date plan including:
  - Measurements of the time required to assemble the team, deploy equipment, reload tapes, etc.
  - A copy of the systems architecture, including system inter-dependencies.

## Disaster Recovery

---

- Lists of software licenses.
- Hardware serial numbers.
- Documentation.
- Rehearse the plan at least once a year.
- Assess reciprocal arrangements vs. internal redundancy.
- Monitor the use of redundant backup systems for routine operations.
- Develop guidelines for diagnostic steps after a disaster, including:
  - An initial assessment of:
    - What caused the failures
    - What are the symptoms
    - The best course of action
  - Familiarization with the data recovery software.
  - Checking the backup tapes.
  - Running a thorough set of hardware diagnostics.
- Develop and maintain up-to-date backup media management, restoration testing and validation procedures.
- Assess new disaster recovery techniques to protect data such as electronic vaulting and server mirroring.

Network recovery involves the execution of technically complex procedures. To ensure a fast recovery, these procedures should always be up-to-date and easily accessible. The availability of such procedures will support effective team training.

## Policies

On June 11, 1996, the Governor's Task Force on Information Resource Management issued 'Technology Policy 96-14 New York State Use of Electronic Mail,' which states: "Agency network administrators and internal control (and/or internal audit) staff are responsible for e-mail security, backup, and disaster recovery."

On January 9, 1997, the Governor's Task Force on Information Resource Management issued 'Technology Policy 97-1 Information Security Policy,' which states: "All systems must have backup and recovery procedures that are documented, maintained and stored off site. The agency should make every effort to test these procedures on an annual basis."