Plan Prerequisites

- Information disaster planning is only effective when it is part of a comprehensive information and records management program. A plan to protect business records is ineffective and needlessly expensive if the majority of the protected records no longer have administrative, legal, fiscal, research or historical value. To reconstruct or salvage outdated or non-essential records is a waste of time and money. More frequently, the lack of approved retention authorizations or not following the retention authorization creates a large body of records that might not be essential or useful to a department. A major disaster is not the appropriate time to conduct a comprehensive review of your records retention authorizations and compliance.

Prerequisite 1: Information is Viewed as a Resource

- Departments that are committed to managing information throughout the total life cycle, from creation or inception, through its use, storage, retrieval, to its final disposition, are more likely to properly place disaster planning in their total management program.

Prerequisite 2: Adequate General Insurance

- An information disaster plan is a form of insurance. Disaster prevention planning is a form of risk assessment. The planning process presupposes that business insurance programs are in place to protect the University's assets and to provide adequate liability protection. Such programs should already be identified and provide protection against certain risks and dangers.
- Risk assessment is a management tool for determining the likelihood of a disaster and its financial impact on the University. A specific dollar amount is placed on each potential disaster by calculating an Annual Loss Expectancy (A.L.E.). The A.L.E. is determined by multiplying the frequency of occurrence by the expected dollar loss per occurrence.
- An information disaster plan complements existing insurance by scrutinizing the University from an information vantage point. The plan identifies specific risks such as building and equipment hazards that can result in flooding to records storage areas, dangerous storage practices that increase the risk of fire near irreplaceable research and development records, and periodic electric storms or tornados that endanger electronically generated vital records. High, medium or low disaster plans have a price tag, but an ounce of prevention is better than a pound of cure.

Prerequisite 3: A Vital Records Program

- In the event of a disaster, recovery can be very costly. It is important that protected, reconstructed, salvaged, and restored records contain information that is essential to the department's continued operation (vital records).
  The identification and protection of essential records represents the gray area where a vital records program and a disaster plan overlap.

Prerequisite 4: A Current Records Retention Schedule

- A vital records program is built upon a detailed records retention schedule -- a comprehensive list of records indicating the length of time each record is maintained in the office area, in the records center, or on electronic media devices and when and if it can be destroyed.
- The retention schedule must precede the vital records protection and disaster recovery plan. This schedule provides necessary information about the location of records, media upon which records are stored, methods of protection, and the value of individual records.

Prerequisite 5: A Sound Records Classification and Retrieval System

- Jumbled, poorly labeled records, whether stored in a bulging file folder, in a disorganized microfilm system, or on a poorly indexed electronic system, significantly increase the cost of disaster planning. The main difficulty is that records are not grouped into workable records series -- a group of identical or related records that are normally used and filed as a unit -- that can be evaluated as a unit for retention scheduling purposes.

Prerequisite 6: An Adequate Security Program

- A general security program for both facilities and information provides the necessary framework to develop an information disaster plan. The following is just a few security elements found in an adequate program:
- Computer passwords/password protection
- Employee identification cards
- Security personnel
- Restricted access areas
- Fire vaults and safes
- Smoke detectors

Summary

Management's commitment to establishing and maintaining a sound records classification and retrieval system, vital records program, current records retention schedules and security is the foundation for building an information disaster prevention and recovery plan.

An information disaster recovery plan is interactive with these prerequisites. Some elements may be fully in place before the disaster planning process begins; others may only be in the elementary stage.

Clearly, any department wanting to protect its recorded information must protect the facility where the records are housed. Unlike "acts of God," disasters caused by building or equipment failure or malfunction can be avoided. Human error or carelessness is frequently the cause of fire, water damage, theft, misinformation, and information loss.

The following represents only a few causes of potential department disasters:

- Smoldering cigarette
- Unlocked window or door
- Negligent storage of flammable materials
- Careless computer keystrokes
- Broken water lines/floods
- Power outages
- Weather (ice, heat & storms)
- Terrorist activities
- Cyber threats

An information disaster prevention and recovery plan begins with a clear, workable definition of disaster. The plan addresses the major types of disasters -- fire, flood, bombing, theft, tornado, etc. It clearly delineates the precise circumstances for activating the disaster recovery procedures. These circumstances are easily defined by identifying the number of hours or days your business operation is shut down by the event, whether recovery is handled in-house or contracted with outside sources