Responsibility for Maintaining Information Technology Backup and recovery Procedures

601.07-1

I. Policy Purpose

As the University of Michigan moves to a more distributed data processing environment, it is necessary to ensure that a localized disaster does not have a major impact on the larger University community. The purpose of this policy is to identify those individuals and units who are responsible for maintaining information technology backup and recovery procedures and to state certain regulations governing those procedures.

II. Policy

Information technology providers at the University of Michigan, including managers who are responsible for the purchase and operation of local area networks, servers, or microcomputers, are responsible for developing, implementing, maintaining, and publishing backup and recovery processes that meet the needs of the users who rely upon their systems. Information technology providers who process mission-critical data are required to develop, implement, maintain, and publish backup and recovery processes that ensure the availability of mission-critical data.

Users of the University of Michigan's distributed systems are responsible for communicating their specific backup and recovery requirements to their information technology provider(s). The backup and recovery requirements for different data and processes vary. Users and service providers must work together to match backup and recovery procedures to the differing levels of data sensitivity and criticality. (For example, for specific guidelines regarding University record data and documents, see SPG 601.8-1, "Identification, Maintenance, and Preservation of Electronic Records Created by the University of Michigan." For electronic mail, see SPG 601.11, "Privacy of Electronic Mail and Computer Files at the University of Michigan.") If a unit uses an external agency for information technology services, the unit must have on file a document that describes the backup and recovery procedures that the agency has committed to provide for the unit.

III. Definition

Mission-critical data—Data that are essential for the ongoing operation of the University of Michigan or for units within the University. Mission-critical data may encompass administrative, research, and instructional data.

IV. Regulations

A. The backup and recovery process must include consideration of at least the following:

1. **Data Availability**—The information processing providers, in consultation with their user community, need to identify the essential data maintained in the environment, particularly that data on which large numbers of users rely or which has a major impact on the operation of the University or the unit. They then need to identify the most likely causes of data unavailability. Finally, they need to identify the backup and recovery requirements for the data.
2. **Application System and Operating System Availability**—The information technology providers, in consultation with their user community, need to identify the application systems and operating systems needed to process the data identified above. They then need to identify the most likely causes of application system or operating system unavailability. Finally, they need to identify the backup and recovery requirements for these application systems and operating systems.
3. **Documentation Availability**—The information technology providers, in consultation with the user community, need to identify which documentation is essential to the ongoing operation of their systems. They then need to identify the most likely causes of documentation unavailability. Finally, they need to identify the backup and recovery requirements for documentation.

4. **Special Equipment Requirements**—The information technology providers, in consultation with their user community, need to identify any special requirements, such as unique hardware, which could not be readily replaced and which would have a major impact on the ability to recover processing capability in the event of the loss of availability of the device. They then should identify the likely reasons for the device to become unavailable. Finally, they should develop a contingency plan for how to handle this situation.
5. **Personnel To Be Notified in the Event of an Unexpected System Outage**—The information technology providers, in consultation with their user community, need to identify personnel who must be notified in the event of a major operational failure or disaster and personnel who must be involved in the recovery efforts.

B. The backup and recovery process must also document the processes for the following:

1. **Data Backup and Recovery**—As the University of Michigan moves to an ever more distributed data processing environment, it becomes necessary to ensure that a localized disaster does not impact the larger University community. Units that maintain operational environments on which other units depend must ensure the availability of the data for which they are responsible and must ensure that the data can be recovered in the event of a localized or far-reaching disaster. To provide for ongoing availability of data, each unit may need to make regular backup copies of the data and to store those backups at both nearby and remote locations. The nearby location will allow for quick access for the recovery of data impacted by a disk drive failure. The remote location will ensure that the data will be recoverable in the event of a major disaster at the data processing site. Units need to develop processes to ensure that data can be recovered in a timely manner.
2. **Application System and Operating System Backup and Recovery**—Data that is stored in machine-readable form generally requires associated application software to read and maintain the data. This software is frequently dependent on the particular implementation of the operating system at the local data processing site. Therefore, information technology providers may need to backup, at both the nearby and remote locations, copies of their application software and the associated operating system software and develop processes to ensure that the backup copies can be used to recover the system.
3. **Documentation Backup**—Documentation may be required to understand successfully the data maintained on the system, the application system, and the operating system environment, and to operate successfully the system and applications. To ensure that the data, application systems, and operating system can be recovered after a disaster, information technology providers must review their documentation to determine which documentation needs to be included in their backup plans.
4. **Special Equipment Requirements**—The information technology providers, in consultation with their vendors, need to develop a plan for quickly replacing any special equipment in the event of a failure of the equipment or of a disaster.
5. **Contact Lists**—The information technology providers must develop and maintain a list of users who need to be contacted in the event of an emergency and a list of essential personnel who need to be involved in the recovery process.

SPG number:
601.07-1

Date issued:
October 30, 1997

Applies to:
All Departments and Units of the University

Owner:
Office of the Provost and Executive Vice President for Academic Affairs

Primary Contact:
Office of the Provost and Executive Vice President for Academic Affairs

Related policies:
Identification, Maintenance, and Preservation of Digital Records Created by University of Michigan
Privacy and the Need to Monitor and Access Records