I.T. Electronic Data Backup Policy

Policy Number:
Owner Department: Information Technology
Effective Date: February 24, 2011
Approved By: President's Council

I. POLICY TITLE

I.T. Electronic Data Backup Policy

II. POLICY STATEMENT

A. The Department of Information Technology is responsible for the backup and recovery of data held on network-accessed information systems.
B. Data stored on an individual's SCNM laptop or desktop computer and not stored on the network is not included in this policy. Each user is responsible for protecting information maintained outside of network storage.

III. POLICY STATUS

New

IV. HISTORY/BACKGROUND

N/A

V. DEFINITION(S)

To backup data is to copy them to another medium (such as tape, DVD, or disk) so that, if the active data are lost, they can be recovered to their original or an alternate location. Backup is primarily intended for disaster recovery, which typically means the data are not intended to be used accessed in real-time.

To archive data is to move them to another medium for long term storage. Archive is intended for the storage of data that do not need to be kept immediately accessible, but which may possibly be needed at some point in the future.

A departmental share is a designated network folder set aside for individual department personnel to store and share data.

VI. PURPOSE

A. The purpose of this policy is to ensure data are protected by providing a mechanism for copying, storing, archiving, and retrieving information.
B. Only data stored on network attached storage devices are protected under this policy.

I.T. Electronic Data Backup Policy

VII. SCOPE/KEY STAKEHOLDERS

SCNM computer network users: Staff, Faculty, Students

VIII. POLICY ITEMS

C. Reasons for backup and archive
   a. The primary reason for backing up data is to keep copies in the event of disaster, for example catastrophic software failure that destroys data, hardware failure of a computer making data inaccessible, or environmental damage to computers such as fire or other natural or unnatural disasters.

D. Central backup of data
   a. SCNM maintains tape backups of data stored on central administrative, academic and infrastructure network servers.

E. Media Rotation Schedule
   a. Data are backed-up Monday through Friday with media stored offsite. Nightly backup media are rotated on a three week cycle, monthly backups are rotated on a 13 month cycle, and an annual backup of Jenzabar's database (Accounting's Year End Close) is stored indefinitely.

F. Departmental networks
   a. Department-based network servers are not permitted.

G. Personal backup of data
   a. Individual users of IT services are responsible for ensuring their data are backed up.
   b. User drives/home directories (U-drives) held on centralized network file servers are configured to back-up nightly. Hence any data residing on or copied to U-drives/home directories at the end of the day are automatically copied to a backup device. Utilizing network storage provides a mechanism for users to backup or archiving data stored on desktop system hard disks.
   c. Backups of U-drives/home directories and departmental shares are taken for disaster recovery purposes. Hence they do not provide security against accidental deletion of individual files. Any file accidentally deleted on the same day that it has been created or modified will not have a backup copy in its latest form and cannot be recovered.
   d. Data critical to SCNM must be kept on network storage devices.
   e. Individual files which have been lost or overwritten will be recovered from central backups provided the information is still accessible, and with the agreement of Information Technology.

IX. RESPONSIBILITY FOR IMPLEMENTATION

Network Administrator

I.T. Electronic Data Backup Policy

X. APPROVAL BODY

President's Council

XI. DATE POLICY APPROVED

February 23, 2011

XII. RELATED POLICIES

Not Defined

XIII. RELATED DOCUMENTS

Not Defined

XIV. DATE EFFECTIVE

February 24, 2011

XV. NEXT REVIEW DATE

As needed

XVI. VERSION CONTROL AND CHANGE HISTORY

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

XVII. POLICY OWNER

Information Technology Department

XVIII. POLICY AUTHOR/CONTACT

Stan Zalewski/Director IT