Title: IT System and Data Backup and Restoration Policy

Purpose

The Information Technology (IT) System and Data Backup and Restoration Policy identifies the steps necessary to protect the availability and integrity of University IT data documented in backup and restoration plans.

Policy Statement

This policy delineates the steps necessary to execute recovery and restoration of University IT systems and data if an event occurs that renders the IT systems and/or data unavailable.

Authority, Responsibility, and Duties

The Office of Information Technology (OIT) is required to implement backup and restoration plans to support restoration of systems and data in accordance with University requirements. These plans should address the following:

1. Secure off-site storage for backup media.
2. Performance of backup only by authorized personnel.
3. Review backup logs after the completion of each backup job to verify successfully completion.
4. Approval of backup schedules of a system by the System Owner.
5. Approval of emergency backup and operations restoration plans by the System Owner.
6. Protection of any backup media that is sent off site (physically or electronically).
7. Authorization and logging of deposits and withdrawals of all media that is stored off-site.
8. Retention of the data handled by an IT system in accordance with the University’ records retention policy.
9. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during legal discovery proceeding.
Definitions

Backup is the process of producing a reserve copy of software or electronic files as precaution in case of primary copy is damaged or lost.

Recovery is the activities beyond the initial crisis period of an emergency or disaster that are designed to return IT systems and/or data to normal operating status.

Restoration is the activities designed to return damaged facilities and equipment to an operational status.

System Owner is the individual designated by the governing UTCC Committee having the responsibility for determining the purpose and function of the IT Resources within the organization for which they are responsible. The Manager has policy level responsibility for managing a segment of the University's IT Resources. Depending on the requirements of the organization, the System Owner may also act as the Data Owner and/or the IT Systems Administrator.

References

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Standard SEC501-01)

APPROVED BY: [Signature]
President
March 17, 2009

Page No: 2