



OIT 62.304: IT System and Data Backup and Restoration

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

IT System and Data Backup and Restoration defines processes and procedures that plan for and execute recovery and restoration of IT systems and information that support essential business functions if an event occurs that renders the IT systems and information unavailable.

II. Purpose

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

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

For every IT system identified as sensitive relative to availability, the University shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data and applications in accordance with University requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.
2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.
3. Performance of backups only by authorized personnel.
4. Review of backup logs after the completion of each backup job to verify successful completion.

5. Approval of backup schedules of a system by the System Owner.
6. Approval of emergency backup and operations restoration plans by the System Owner.
7. Protection of any backup media that is sent off-site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.
8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.
9. Retention of the data handled by an IT system in accordance with the University's records retention policy.
10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.
11. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.
12. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with the University's Continuity of Operations Plan.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.