



## OIT 62.302: Continuity of Operations Planning

**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

Continuity of Operations Planning 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 University Continuity of Operations Planning (COOP) requirements are outside of the scope of this Policy. This policy addresses only the IT disaster recovery components of the COOP for IT systems and data. The University should consult the Continuity of Operations Planning Manual published by VDEM for COOP guidance.

These IT disaster recovery components of the COOP identify the steps necessary to provide continuity for essential University IT systems and data.

### III. Scope

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

### IV. Requirements

NSU shall:

1. Designate an employee to collaborate with the University Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery (DR) planning activities.

**Note:** Designation of an agency COOP coordinator is included in the COOP planning requirements issued by VDEM.

2. Based on BIA and RA results, develop IT disaster components of the University COOP which identifies:
  - a. Each IT system that is necessary to recover essential business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and
  - b. Personnel contact information and incident notification procedures.

**Note:** If the COOP contains sensitive data, those components with sensitive data should be protected and stored at a secure off-site location.
3. Require an annual exercise (or more often as necessary) of IT DR components to assess their adequacy and effectiveness.
4. Require review and revision of IT DR components following the exercise (and at other times as necessary).

## **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.