



## **OIT 62.303: IT Disaster Recovery Planning Documentation**

**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 Disaster Recovery 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**

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that support University mission requirements. These steps lead to the creation of an IT Disaster Recovery Plan (DRP).

### **III. Scope**

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

### **IV. Requirements**

NSU shall:

1. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions and dependent business functions.
2. Require approval of the IT DRP by the Agency Head.
3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.
4. Establish communication methods to support IT system users' local and remote access to IT systems, 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.