



## **OIT 62.604: Protection of Sensitive Information on Non-Electronic Media**

**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**

University employees and other personnel who have access to sensitive and confidential University information that may be stored or transmitted on non-electronic media, such as the spoken words, paper documents, white or black boards, photographs, etc., should take appropriate steps to protect such information and properly destroy it, when it is no longer needed.

### **II. Purpose**

The purpose of this policy is to provide users with relevant guidance concerning the protection and destruction of non-electronic information.

### **III. Scope**

This policy applies to NSU employees and other personnel (i.e. supporting vendors, consultants, etc.) who have access to sensitive and confidential University information.

### **IV. Recommendations**

The following recommendations apply to non-electronic University information:

1. While in use, limit access based on a need to know basis by physically controlling access. For example, sensitive documents printed to a global printer should be retrieved without delay.
2. While not in use, store in a secure location with appropriate physical controls.
3. When no longer needed, securely destroy using appropriate destruction methods such as erasing white or black boards and shredding paper.

### **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.