



OIT 62.803: Information Security Awareness and Training

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

Information security awareness and training is required to provide all IT system users with appropriate understanding regarding University Information Security Policies and acceptable use requirements for IT systems and data.

II. Purpose

The Security Awareness and Training policy identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

III. Scope

This policy applies to NSU employees and other personnel who have access to University information technology systems.

IV. Requirements

The University shall:

1. Include any University-specific information security training requirements in the agency information security awareness and training program.

Example: A department that processes data covered by the Family Educational Rights and Privacy Act (FERPA) must have an information security awareness training program that addresses specific FERPA data security requirements.

2. Require that all IT system users, including employees and contractors, receive information security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.

3. Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.

Example: University employees and contractors who are members of the Disaster Recovery Team or Security Incident Response Team require specialized training in these duties.

4. Implement processes to monitor and track completion of information security training.
5. Require information security training before (or as soon as practicable after) IT system users receive access rights to the agency's IT systems, and in order to maintain these access rights.
6. Develop an information security training program so that each IT system user is aware of and understands the following concepts:
 - a. The University's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
 - b. The concept of separation of duties;
 - c. Prevention and detection of information security incidents, including those caused by malicious code;
 - d. Proper disposal of data storage media;
 - e. Proper use of encryption;
 - f. Access controls, including creating and changing passwords and the need to keep them confidential;

Note: It is considered best practice not to base passwords on a single dictionary word. It is strongly recommended that system users be educated not to base passwords on a single dictionary word.

- g. University acceptable use policies;
- h. University Remote Access policies;
- i. Intellectual property rights, including software licensing and copyright issues;
- j. Responsibility for the security of University data;
- k. Phishing; and
- l. Social engineering.

Note: Over a period of years, security awareness training should include the concepts above based on the needs of the University relative to the sensitivity of the University's data and IT systems.

7. Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.

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.