Purpose

The Security Awareness and Training identifies the steps necessary to provide Information Technology (IT) system managers, administrators, and employees with awareness of IT system security and their responsibilities to protect University IT systems and data.

Policy Statement

The IT Security Awareness Training program is mandatory for all University employees, students, and contractors.

Authority, Responsibility, and Duties

The Virginia Information Technology Agency (VITA) Information Security Standard (ITRM Policy SEC 501-01) requires the University to establish a baseline for IT security controls, which will allow the University to accomplish its mission in a safe and secure environment. The University is instituting a Security Awareness Training program for all University employees, student, vendors, contractors, and business partners to comply with this standard.

The Office of University Technology and Human Resources shall:

1. Implement, maintain, and provide on-going information technology Security Awareness Training using various training delivery techniques in awareness sessions, use email distribution for security awareness communications, and publish a security web site to promote and reinforce good security practices, University policies and procedures, and employee responsibilities.

2. Establish accountability and monitor compliance by implementing an automated tracking system to capture key information regarding program activity (i.e. courses, certificates, attendance, etc.).

3. Implement formal evaluation and feedback mechanism to address quality, scope, deployment method (e.g., web-based, onsite, offsite), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Faculty, Faculty Administrators, Staff, Contractors, Vendors, and Business Partners who use University IT systems will be required to:

1. Complete an annual online Security Awareness Training course every twelve (12) months. All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from date of hire or prior to receiving access to the University’s IT systems and data.
2. Sign an "Acceptable Use Policy and IT Acceptable Use Standards and User Acknowledgement Agreement" which acknowledges that they are fully aware of security best practices, their roles in protecting the University's information technology systems and data. Access to University computer technology will not be granted without this agreement.

Students (i.e. full-time, part-time, and transfer) are required to:

1. Complete the online Security Awareness Training course prior to receiving access to the University's IT systems and data.

2. Sign an "Acceptable Use Policy and IT Acceptable Use Standards and User Acknowledgement Agreement" which acknowledges that they are fully aware of security best practices, their roles in protecting the University's information technology systems and data.

Supervisors, Managers, Deans, and Directors are required to:

1. Ensure each employee under his/her supervision has attended and completed the Security Awareness Training and should include the training as a part of the employee's annual performance evaluation.

2. Maintain a copy of each employee's Security Awareness Training certificate in the department's personnel file and forward a copy of the employee's certificate to the Human Resource Department for the employee's personnel file.

Definitions

A. **Information Assets** are defined as (1) All categories of automated information, including (but not limited to) records, files, and data bases; and (2) information technology facilities, equipment (including personal computer systems), and software owned or leased by the University. This includes all University IT systems and data.

B. **Security Awareness Training (SAT)** is a method to inform users in the importance of promoting and protecting information technology systems and assets. SAT is a training course that teaches security key concepts and best practices, such as creating a strong password, protecting mobile data, following acceptable use policy, and reporting security incidents.
Virginia State University
Policies Manual

Title: Security Awareness Training Policy
Policy: 6530

References

National Institute of Standards and Technology (NIST): Technology Administration
Building an Information Security Awareness and Training Program

Virginia Department of Human Resources Management (DHRM):
Use of Internet and Electronic Communication Systems (Policy 1.75)

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Policy SEC500-02)

Virginia State University (VSU):
Policy 6520: Acceptable Use Policy
Policy 6420: Electronic Records and Retention Policy
Policy 6110: IT Resource Security Policy
Policy 6640: Network Monitoring Policy
Policy 6310: Banner Security Policy
Policy 6630: Data Breach Notification Policy
Policy 6620: IT Security Handling Policy
Policy 6710: IT System and Data Backup and Restoration Policy

APPROVED BY: [Signature]
President
Date: 1/28/08

Revision Date: January 28, 2008