Title: Security Awareness and Training Policy Policy: 6530

Purpose

The purpose of the Security Awareness and Training policy is to identify the steps necessary to provide Information Technology (IT) system managers, administrators, and employees with awareness of IT system security and their training responsibilities in regards to University IT systems and data. This policy establishes the minimum requirements for the Security Awareness and Training controls and is intended to meet the control requirements outlined in the current Awareness and Training section and control family of SEC501-09.

Scope

In accordance with SEC501, VSU provides Security Awareness and Training for all VSU faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors and business partners prior to accessing VSU's data and information technology resources and annually, thereafter or more frequently if required to address environmental changes. VSU's Security Awareness and Training addresses roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The training also includes general information security training, role-based training, system specific training and general awareness.

Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as, the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests. Refer to Information Security Policy 6110 for IT Security Program roles and responsibilities.

A. All University Staff and Employees

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. Additional Security Awareness Training may be required by all employees at other intervals when the IT infrastructure or environment changes and training is necessary.
3. Read the "Acceptable Use Policy" and sign the "IT Acceptable Use Standards and User Acknowledgement Agreement" which acknowledges that he/she is fully aware of security best practices and his or her associated roles in protecting the University's information

technology systems and data. This agreement acknowledgement is in the University Security Awareness training portal. Access to University computer technology will not be granted without this fully signed and ratified agreement in place.

B. 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.
3. Managers will ensure that VSU faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors and business partners who manage, administer, operate, or design IT systems, receive additional role-based information security training as deemed appropriate and that is commensurate with their level of expertise, roles and responsibilities.

C. System Owners

1. Facilitate and participate in practical cybersecurity training exercises on an ad hoc basis that simulate cyber-attacks and threats for situational and enterprise readiness.
2. Complete yearly role based training (or more frequent intervals based upon enterprise needs) and maintain records of said training.

D. Privileged and/or Administrative Users

1. Facilitate and participate in practical cybersecurity training exercises on an ad hoc basis that simulate cyber-attacks and threats for situational and enterprise readiness.
2. Complete yearly role based training (or more frequent intervals based upon enterprise needs) and maintain records of said training.

E. Data Owners

1. Complete yearly role based training (or more frequent intervals based upon enterprise needs) and maintain records of said training.

General Policy Statements

1. This Security Awareness and Training policy applies to all University employees (permanent, temporary, contractual, faculty, and administrators) who are responsible for the development, coordination, and execution and use of VSU information technology resources to conduct University business and to transmit sensitive data in the performance of their jobs.
2. It is the policy of VSU that the Technology Services department will implement information security awareness and training best practices. At a minimum, these practices include the following components:
   a. 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.

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

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

3. All University employees (permanent, temporary, contractual, faculty, and administrators) must be aware of and understand the following IT principles through training (either in-person or online):

   a. Protection of IT systems and data;
   b. Separation of duties and what that means to the user;
   c. Prevention and detection of security incidents;
   d. Disposal of data storage medium;
   e. Use of encryption;
   f. Access controls, including the password policy of the University and the need for confidentiality of passwords;
   g. Acceptable use policy;
   h. Remote access policy;
   i. Software licensing and copyright issues;
   j. Responsibility of protecting Commonwealth of Virginia data;
   k. Phishing;
   l. Social engineering and
   m. Least privilege principles.

4. A variety of methods will be used to deliver Security Awareness and Training to VSU faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors and business partners regularly throughout the year. Methods of delivery include, but are not limited to, posters, newsletters, email messages, active drills, online, oral presentations and events consistent with the Information Security Standard (SEC501-09).

5. The CISO will oversee VSU's Security Awareness and Training program, including development, implementation, and testing.

6. The CISO or designee will coordinate, monitor and track the completion of the Security Awareness Training for all VSU faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors and business partners and report incomplete training to the respective senior executive, manager or accountable person.

7. The CISO has the ability to impose sanctions against non-compliant users for failure to complete the training including, but not limited to: disabling accounts, reporting to Human Resources and discontinuation of access to IT services.
8. Individual training records will be retained as defined by the agency's records retention policy.

Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

Acronyms

AH:	Agency Head/President of VSU
CCIO:	COV Chief Information Officer
CCISO:	COV Chief Information Security Officer
CIO:	Chief Information Officer of VSU
CISO:	COV Chief Information Security Officer of VSU
COV:	Commonwealth of Virginia
CSRM:	Commonwealth Security and Risk Management
HR:	Human Resources
IT:	Information Technology
ITRM:	Information Technology Resource Management
SEC501:	Information Security Standard 501
TS:	Technology Services
VITA:	Virginia Information Technologies Agency

References

Virginia Department of Human Resources Management:

Policy 1.60 Standards of Conduct (4/16/08, 6/1/11)
Policy 1.75 Uses of Electronic Communication and Social Media (8/01/01, 3/17/11)

Virginia Information Technology Agency (VITA):

Information Security Standard (SEC 501-09) (02/20/2015)

Approval By: _____ Date: 5/10/16
President