Purpose

The Security Awareness and Training Policy establishes the requirements to assist Information Technology (IT) system managers, administrators, and users of VSU systems and data the steps to ensure that university systems and data are appropriately safeguarded. Our faculty, staff and students are the frontline to protecting the university's data assets and this policy will assist at providing consistent guidance and overall approach to security awareness.

Scope

VSU provides Security Awareness Training for all university faculty, staff, deans, vice presidents, interns, managers, senior managers, board members, contractors and business partners prior to assessing VSU's data and information technology resources and annually. The training will address roles, responsibilities, management commitment, proper disposal of data storage media, coordination among organizational entities and compliance. (Note: Special focus is given to sensitive system and data concerns.)

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.

A. 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 IT infrastructure environment changes.
3. Read the "Acceptable Use Policy" and electronically sign the 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.

A. 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, role and responsibilities.

B. 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 annual role based training (or more frequent intervals based upon enterprise needs) and maintain records of training.

C. System Administrators

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 annual role based training (or more frequent intervals based upon enterprise needs) and maintain records of training

D. Data Owner

Complete annual role based training (or more frequent intervals based upon enterprise needs) and maintain records of training

E. Information Security Officer

1. Aligns the University's Security Awareness Program with the Commonwealth's SEC 501-09.1 Standard and industry best practice.
2. Oversees VSU's Security Awareness and Training program, including development, implementation and testing.
3. Coordinates, monitors and tracks 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
4. Develops the role based training and maintains records of training for entire program

General Policy Statements

1. All University employees (permanent, temporary, contractual, faculty, and administrators) who use VSU information technology resources to conduct University business and to transmit sensitive data in the performance of their jobs must take security awareness training prior to using VSU systems, when required by information system changes; and annually thereafter.
2. In an effort to educate VSU system users in understanding their responsibility in safeguarding systems and data, security awareness training will include the following concepts:

a. The agency'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;
g. Agency acceptable use policies;
h. Agency Remote Access policies;
i. Intellectual property rights, including software licensing and copyright issues;
j. Responsibility for the security of COV data;
k. Phishing;
l. Social engineering; and
m. Least privilege.

3. Role specific training will be provided to the following specialized users (System Owners, Data Owners, and Security Administrators). Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. This training will also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to the university.
4. To ensure compliance with the annual security awareness training, training will be documented and monitored for individual information system security training activities including basic security awareness training and specific information security training (i.e. role based training); and
5. Training records to support training activities will be retained for period as defined by the university'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.

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.).

References

Virginia Information Technology Agency (VITA):

Information Security Standards (SEC501-09.1) (12/08/2016)
IT Security Audit Standard (SEC502-02.3) (12/08/2016)

9/6/17

Approval By: _____ **Date**_____
President