Title	Policy ID:	
651-1_VSC_Security_Awareness	651-1	
	Version:	Date:
	1.0	**9/10/2018**

1. Purpose

1.1. This policy specifies an information security awareness and training program to inform and motivate all users regarding their information risk, security, privacy and related obligations at the Vermont State Colleges System.

2. Scope

2.1. This policy applies to all users of VSCS resources and data including but not limited to faculty, staff, students, and third-party contractors whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior). It applies regardless of whether users utilize electronic systems and/or networks, since everyone is expected to protect all forms of information assets including electronic data, written materials/paperwork and intangible forms of knowledge and experience.

3. Policy

3.1. Background

3.1.1. Effective information security requires the awareness and proactive support of all users, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and frauds, for example, which directly target vulnerable humans rather than IT and network systems.

3.1.2. Lacking adequate information security awareness, users are less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information in danger through ignorance and carelessness.

3.2. Detailed policy requirements

3.2.1. An information security awareness program should ensure that all users achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms plus generally held standards of ethics and acceptable behavior.

3.2.2. Additional training is appropriate for users with specific obligations towards information security that are not satisfied by basic security awareness, for example HIPAA, PCI, FERPA, etc.

3.2.3. Security awareness and training activities should commence within 30 days after users join the organization. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness of current issues and challenges in this area.

3.2.4. Where necessary, security awareness and training materials should suit their intended audiences

3.2.5. CISO/ISO sanctioned exercises are permitted to assess the current state of information security awareness at the VSCS.

3.3. Responsibilities and accountabilities

3.3.1. The Chief Information Security Officer/Information Security Officer (CISO/ISO) is accountable for running an effective information security awareness and training program that informs and motivates users to help protect the organization's information assets, and third-party information (including personal data) in our care.

3.3.2. Managers are responsible for ensuring that their staff and other users within their remit participate in the information security awareness, training and educational activities where appropriate.

3.3.3. Users are personally accountable for complying with applicable policies, laws and regulations at all times.

3.3.4. Internal auditing is authorized to assess compliance with this and other corporate policies at any time.

4. References

5. Definitions

5.1. VSCS – Vermont State Colleges System

6. Revisions

Date	Revision	Approval	Signature
9/10/2018	Original Draft	M. Knapp	
11/15/2019	Approved by ITC	G. Malinowski	
11/18/2019	Approved	M. Knapp	
11/18/2019	Approved	D. Bazluke	