

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Personnel Security – *Security Awareness and Training Program***

In accordance with the [COV ITRM 501-01](#), a security awareness and training program must be implemented for all managers, administrators, and users to focus attention on security and produce relevant and needed security skills and competency. Further, the security awareness and training program must provide technical training for all VCCS employees involved in the management, administration, operation, development, or use of information systems. [SVCC employee participation is mandatory; System Owners should not approve access for users that do not meet training requirements.](#)

The standards developed in this document define minimum requirements and recommendations in improving information technology security awareness and developing the necessary skills and knowledge to assist all System Office and College users in performing their job responsibilities in a secure and accountable manner. The following requirements and recommendations are provided to assist with compliance of the Commonwealth of Virginia (COV) Information Technology Resource Management Standard, [COV ITRM 501-01](#) standards for security awareness and training. The VCCS Information Security Officer and College Information Security Officers should be assigned the responsibility for developing, implementing, testing, training, monitoring attendance, and periodically updating the Security Awareness and Training Program. Mr. Will Hamilton, IT Security Analyst and ISO is responsible for managing the Security Awareness and Training Program at SVCC. Administrative leadership, at the System Office and college level, should be provided to convey the importance of the Information Technology Security Awareness and Training Program. Security awareness focuses attention on a security issue or set of issues. Security training is more formal and the goal is to build knowledge and skills at the appropriate level to facilitate job performance. The combination of security awareness and training are implemented to support individual accountability which improves overall information technology security.

**Requirement:** Develop a formal information security awareness and training program to include specific training requirements. SVCC uses the Managed Ongoing Awareness Tools (MOAT) program by Awareity to meet this requirement. Employees may be exempt from security awareness and training if exceptional circumstances are indicated and documented by their supervisor. The exception must be approved by the President's Staff, signed by a representative thereof, and by the college ISO. This information will be recorded on the Personnel Security: *Security Awareness and Training Program*, security

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Personnel Security – *Security Awareness and Training Program***

awareness compliance exemption form. (Attachment H 2.1) The completed form will be maintained in the employees personnel file.

**Requirement:** SVCC employees receive annual security awareness training via the MOAT mechanism. Refresher, updated, or special situational training as technology, System Office, or college environments change will be held as appropriate, and at a minimum annually.

**Requirement:** SVCC monitors and documents attendance at all security related training by using electronic reporting included in Managed Ongoing Awareness Tools (MOAT). Each user has an assigned account that uniquely identifies them in the database which records and timestamps all activities for said user.

**Requirement:** Construct information security training programs so that all employees are aware of and understand the System Office and SVCC policy for protecting information and information systems, separation of duties concepts, restriction of system access by employees engaged in key operating and programming activities, prescribed roles in incident response, configuration management, and continuity of operations, password management, the importance of monitoring log-in success/failure and reporting discrepancies, and handling of information types (in particular the handling of information classified as sensitive or critical) specific to SVCC. Again, MOAT addresses all these issues.

**Requirement:** New SVCC employees receive and complete security training within the first three months of employment, via MOAT. Adjunct faculty, special needs employees, short term employees, and third parties doing IT work on behalf of SVCC, will receive security awareness training via the SVCC website by completing the Personnel Security: Security Awareness and Training Program, *security awareness training for third parties and short term employees* form. (Attachment H 2.1) The completed form will be maintained in the employees personnel file.

**Requirement:** Establish and maintain specialized or advanced training so that all individuals involved in the management, administration, operation, or design of information systems know how to incorporate proper security practices and how to fulfill their security responsibilities. These requirements are met by using training opportunities afforded SVCC by the VCCS, Virginia Tech, VA SCAN, the SANS institute, and other

---

## SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

### **Personnel Security – *Security Awareness and Training Program***

applicable training providers. It will be the responsibility of the individual employee's supervisor to ensure compliance with this requirement. SVCC makes additional security awareness training available to all employees at the following locations:

<http://www.southside.edu/student/infosecurity/tipofmonth.asp>

[http://inside.southside.edu/security/security\\_awareness.asp](http://inside.southside.edu/security/security_awareness.asp)

**Requirement:** SVCC will make available information technology security training programs that commensurate to the level of expertise required for the system components and information resources for which the college personnel are responsible. The program shall include content that enables the individual to identify and evaluate threats, vulnerabilities and risks specific to those components and resources. The program must further include content regarding technical alternatives, methods, and standards which represent best practices appropriate to those components and resources, and which can be utilized to effectively implement safeguards as appropriate. MOAT will be deployed; Levels of training will be determined, initiated, and documented by the employee's supervisor. The supervisor may use a guideline the employees' level of IT access as determined by the Logical Access Control: *Account Management* and the Personnel Security: *Access Determination and Control* standards and all applicable forms and procedures. (Section E 1 and Attachment E 1.1, H 1 and H 1.1 respectively)