
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Threat Detection*

Threat Detection Plan

In accordance with the [COV ITRM 501-01](#), threat detection policies must be implemented to ensure the Systems Office and colleges are aware of threats and establish procedures to prevent attacks. A threat is a harmful act such as the deployment of a virus or an illegal network incursion. Practices for implementing intrusion detection and prevention assist in minimizing the effects of threats to IT systems and data.

The System Office and Colleges must designate an individual who is responsible for the threat detection plan. The plan should include the development, acquisition, implementation, testing, training, and maintenance of threat detection activities. The person responsible for recommending a threat detection plan to SVCC President's Staff is Mr. Will Hamilton, Information Technology Systems Security Analyst, and ISO. Mr. Hamilton's EWP will reflect this responsibility. SVCC President's staff must approve the plan and all associated documentation.

In order to meet the requirements of the [COV ITRM 501-01](#), an Incident Response Team was formed to assist in the Threat Management and Threat Detection processes. The team members are from different departments as specified in requirement 1 of the Threat Management: *Incident Handling* standard, and are listed in (Attachment I 2.1).

The college has implemented various types of threat detection techniques, including firewalls, IDS, IPS, and edge router perimeter security. The IT members of the Incident Response Team, (network administrators) have the responsibility for deployment, testing, designating trainees, maintaining, and documenting all of these threat detection activities. In addition, the plan director will make suggestions as to how these activities should be completed and give completion dates for various components of the plan.

In compliance with the VCCS Threat Management: *Threat Detection* standard, threat detection training is provided to all personnel to whom it applies. The members of the Incident Response Team will make recommendations as to the personnel who should receive training from their areas of responsibility; these recommendations must be approved by the employee's supervisor. Training will be done by vendor recommended trainers, and will be done prior to any equipment installation. It is recommended that the plan director/ISO attend this training as well. Additional training may be required as needed to update employee's skills as technology changes, with no more than a

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Threat Detection*

Threat Detection Plan

maximum two years between training sessions, or as deemed necessary and proper by the college's administration. All training will be documented and maintained by the employee's supervisor.

Another requirement of the VCCS Threat Management: *Threat Detection* standard is that a review of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) logs must be conducted to detect new attack patterns. Event logs on servers and other mission critical devices will be monitored for suspicious activities as is reasonable and not to impede normal business functions. Reviews of all logging must be conducted as quickly as practicable to ensure mitigation measures are developed and implemented to minimize or prevent future threats. The IT members of the Incident Response Team (network administrators) will be responsible for implementation and documentation of these activities as per the Threat Management: *IT Security Monitoring and Logging* standard, with additional comprehensive annual reviews done prior to June 15.

The final requirement of the Threat Management Plan is that the System Office and Colleges must maintain communication with organizations that can provide information about new attack types, vulnerabilities, and mitigation measures, and that these measures be tested, and implemented as soon as possible and as not to impede normal business functions. SVCC has maintenance contracts with the vendors of all the threat detection appliances which it has deployed. As such, the college receives constant updates as to vulnerabilities or exploits and recommended remedies for the same. The members of the Incident Response Team will be responsible for dissemination of information regarding new attack types, vulnerabilities, and mitigation measures to appropriate personnel in their areas of responsibility. Additionally, the following resources may be used by SVCC:

Cyber Security Alerts: <http://www.us-cert.gov/cas/alerts/>.

Cyber Security Tips: <http://www.us-cert.gov/cas/tips/>.

Cyber Security Bulletins: <http://www.us-cert.gov/cas/bulletins/>.

Microsoft Security Advisor: <http://www.microsoft.com/security/default.mspx>

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Threat Detection*

Threat Detection Plan

The SVCC Information Technology Threat management, Threat Detection document and all other associated documentation are approved as given in Section I1 of the SVCC Security Plan.

1. Date Reviewed: _____

2. Reviewed By: SVCC President's Staff _____

3. Approved By: _____

SVCC President: Dr. John Cavan