
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *IT Security Monitoring and Logging*

In accordance with the [COV ITRM 501-01](#), IT Security Monitoring and Logging policies and procedures must be implemented to ensure the Systems Office and colleges are taking appropriate measures to monitor and record IT system activity.

Logging of security and other system related events assists in the investigation of security related incidents. Logging capabilities may be at the application or system level or both.

Requirement:

Colleges must designate individuals who are responsible for the development and implementation of logging capabilities and the supporting policies where applicable. This includes developing procedures for reviewing and administering the logs. At SVCC, the IT Network Administrators are tasked with this responsibility the employee's EWP should reflect these responsibilities.

Requirement:

SVCC must enable logging capabilities on **all (Jan 2010 Revision)** IT systems and applications where practicable and does not impede the performance of the IT system or otherwise impact the Systems Office or College business practices. **At a minimum, logs will include:**

- a. The user ID associated with the event.
- b. The time the event occurred. **(Jan 2010 Revision)**

Alternate security procedures (monitoring and logging at the firewall, IDS, etc. for example) must be documented to ensure IT security monitoring and logging is maintained at an appropriate level to protect against threats. IT Network Administrators will determine the logging levels and maintain all necessary documentation of the same.

Requirement:

Event logs should be monitored so that quick reactions to an attack are implemented. If other automated tools are in place, a comparison of the event must be made to provide a clear picture of what has occurred. Once the suspicious activity has been identified, alert notifications must be provided to the appropriate staff. IT Network Administrators monitor logging as per requirement 2 above. Alert notifications are given by the IT Network Administrator to appropriate staff as is reasonable and proper for the situation,

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *IT Security Monitoring and Logging*

and per the Threat Management: *Incident Handling*, Incident Response Plan (Attachment I 2.1) if necessary.

Requirement:

SVCC must specify the type of actions a particular program can take, based on the possible security implications, when suspicious or malicious traffic is detected. For example, a passive IDS may detect and alert a system administrator who will then make a decision to take action to respond accordingly. A reactive IDS may detect, alert, and take a pre-defined action to respond to the threat. In either scenario, the actions must be specified. This may include blocking traffic once a particular time has elapsed, shutting down the system, and alerting appropriate staff. IT Network Administrators at SVCC are tasked with the responsibility of meeting this requirement. The SVCC IT Staff will maintain documentation with specific information as to the nature of the suspicious traffic, the mechanism by which it was detected, and the actions taken by the detecting device(s) upon such detection.

Requirement

The use of keystroke logging shall be prohibited at the System Office and individual colleges, except when required for security investigations and approved in writing by the Agency Head. (Jan 2009 Revision)

Requirement (Jan 2010 Revision)

Prohibit the installation or use of unauthorized monitoring devices.

Note: For investigative purposes, the CISO or ISO has the responsibility to authorize monitoring or scanning activities for network traffic; application and information access; user commands; email and Internet usage; and message and information content for IT systems and data. As noted above, the use of key-stroke logging is prohibited, except when required for security investigations and a documented business case outlining the need and unmitigated risk has been approved in writing by the Agency Head. The CISO and the ISO shall notify each other when appropriate.