
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management - *Incident Handling*

In accordance with the [COV ITRM 501-01](#), incident handling is necessary to detect incidents, minimize loss, mitigate weaknesses and restore System Office and College resources promptly and efficiently.

Incident handling involves having the necessary tools and resources in place to appropriately handle an incident. The SANS Institute defines an incident as “An adverse event in an information system and/or network, or the threat of the occurrence of such an event. Incident implies harm or the intent to do harm.”

Note: The CISO, in conjunction with the Agency Head through the agency ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of laws, regulations, policies or standards in order to preserve evidence that might be utilized in forensic analysis of a security incident. (Jan 2010 Revision)

Requirement:

SVCC must designate an Incident Response Team (Attachment I 2.1) that includes personnel with the appropriate expertise and authority to respond to each phase of an incident report. This may include:

- Information Technology employees with the expertise in incident handling procedures.
- Public Relations, College Relations, or similar department who is authorized to communicate with the media if required depending on the nature and impact of the incident.
- Human Resources personnel who are authorize to assist in disciplinary or employee relations.
- Security Services or Campus Police offices that may need to make reports internally or externally in physical breach or law breaking situations. These offices may also be needed in situations that require law enforcement intervention (i.e., removal of a disgruntled employee).
- Facilities Management personnel who may be needed to access physical office locations during an incident (i.e., to obtain a workstation from a locked office).
- Business Continuity Planning or Continuity of Operations Planning personnel may need to be aware of incidents that may require a review of risk assessments and continuity of operations plans.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management - *Incident Handling*

Requirement:

SVCC must minimize loss or theft of information by identifying controls to deter and defend against incidents. This includes proactive measures to defend against new forms of attacks. Controls must be identified and may include:

- Patch management programs to assist in system administration.
- Host Security configurations that comply with the principle of least privilege, allow users to change default settings, provide warning banner displays, enable auditing, and similar host security provisions.
- Network security configurations that deny all activity not specifically permitted.
- Malicious code prevention software to detect and stop malicious code at the host, server, and application level.
- Security Awareness and Training standards and procedures that make end users aware of the appropriate use of networks, systems, and applications.
- **Technical training for information technology staff so they can properly maintain their system, network, or application.** (Removed in the COV ITRM 501-01 July 2007 Revision)

This requirement is addressed in the Threat Management: *Incident Handling*, Incident Response Plan (Attachment I 2.1)

Requirement:

Incidents should be handled based on the critical nature of the affected resources and on the current and potential effects of the incident. The information obtained in the Business Impact Analysis and Risk Assessment processes will assist SVCC in establishing written guidelines for prioritizing the handling of incidents, how quickly the Incident Response Team must respond to the incident, and what actions should be performed for the incident. These procedures are outlined in the Threat Management: *Incident Handling*, Incident Response Plan (Attachment I 2.1)

Requirement:

SVCC must establish written guidelines that include mitigation strategies for each major type of incident as set forth in the Threat Management: *Incident Handling*, Incident Response Plan (Attachment I 2.1)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management - *Incident Handling*

Mitigation strategies vary based on the type of incident, and are listed in Attachment I 2.1. Part of mitigation procedures must include decisions to shut down a system, disconnect it from a network, etc. A decision may be altered by the Incident Response Team based on the need to gather evidence of the incident and the team must be willing to accept any risks involved in delaying a decision.

Requirement:

The VCCS Information Technology Services Office will coordinate security incident reporting for the System Office and Colleges to comply with the Code of Virginia [§ 2.2-603.G](#), which describes the reporting requirements agency's must follow. The Systems Office and Colleges must reference the [VITA Guidance on Reporting Incidents](#) and adhere to these guidelines when reporting incidents **to the VCCS Information Technology Services Office** via [Issue Trak](#) (Issue Type: Network – Abuse) or Abuse@vccs.edu. At a minimum, the information below is required when reporting an incident. The System Office and Colleges are encouraged to complete the Incident Reporting Form and include this as an attachment to the Issue Trak or Abuse@vccs.edu email.

- Date and time of the incident
- Incident description
- Impact of the Incident
- Severity of the attack (high, medium, low)
- Steps taken to respond to the attack
- Names of others who have been notified

All incidents must be reported only through channels that have not been compromised. If either of the above reporting methods are compromised, verbal or face-to-face reporting may be used.

Requirement:

The System Office and Colleges must have established procedures for how team members will conduct the investigation, how evidence will be preserved, and how the forensic analysis will be conducted. This may include recording all facts, documenting system events and telephone conversations. This may also describe how team members will work together to ensure viable results in researching and documenting incidents.

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

Threat Management - *Incident Handling*

Forensic analysis may be conducted using forensic software or by manually reviewing files and generating reports. The above two requirements are addressed in the Threat Management: *Incident Handling*, Incident Response Plan and associated forms.

(Attachment I 2.1)

Each agency shall document IT security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling. (Jan 2009 Revision)