
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Incident Response Plan

In order to meet the requirements of the [COV ITRM 501-01](#), and the VCCS Threat Management: *Incident Handling* standards, SVCC drafted an Incident Response Plan (IRP). 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.”

The objective of the Incident Response Plan is to define the possible incidents that may occur in the Southside Virginia Community College (SVCC) information technology system and define the procedures for handling each type of incident. SVCC IT staff and Incident Response Team will reference the COV ITRM SEC510-00 IT Security Threat Management Guideline (Attachment I 2.1) for guidance in responding to and recovering from threats against COV owned IT resources.

SVCC College has established a Help Desk for users to report all information technology problems. College users should report all incidents to the College Help Desk Daniel: ext. 2041, Christanna: ext. 1078. The objective of the Incident Response Plan is to define the possible incidents that may occur and define the procedures Information Technology staff (IT) should follow for handling each type of incident. This document should be reviewed at least once a year to determine what if any changes are required.

The first step in the process is designating 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. These personnel 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

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Incident Response Plan

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.

The next step is to identify and implement controls to deter and defend against incidents. This includes proactive measures to defend against new forms of attacks. The following controls are in place to assist in recognizing and mitigating different incidents.

- Frequent and as needed IDS, IPS, IOS, OS, vulnerability, and exploit updates from vendors to assist in system administration.
- Host security configurations that comply with the VCCS Logical Access Control: *Account Management* and Personnel Security: *Access Determination and Control* standards.
- Network security configurations (firewalls, IDS, IPS, perimeter router) that deny all activity not specifically permitted. Monitoring and logging all appropriate network activities as per the Threat Management: *Security Monitoring and Logging* standard. (Section I 3)
- Malicious code prevention software to detect and stop malicious code at the host, server, and application level. The College uses Norman and Symantec Antivirus software to protect hosts and servers.
- Security Awareness and Training standards and procedures that make end users aware of the appropriate use of networks, systems, and applications. SVCC uses MOAT Security Awareness Training.
- Technical training for information technology staff so they can properly maintain their system, network, or application is available and ongoing and is a budgeted item in the IT department's annual expenditures. Each IT staff member will maintain documentation as to annual training attended.

The third requirement of the IRP is that incidents should be handled based on the critical nature of the affected resources and on the current and potential effects of the incident.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Incident Response Plan

The information obtained in the Business Impact Analysis and Risk Assessment processes will assist the System Office and Colleges 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. SVCC has prioritized the incident handling process as follows: All incidents involving mission critical applications or processes as identified during the BIA and RA process (see BIA form 3, Attachment B 2.1c) will be given priority over all other classifications of incidents. The remaining incidents will be classified and prioritized as follows: Global incidents (those that affect the entire enterprise) will be addressed first. For example, a compromised or defective enterprise server, router, firewall, switch etc. Systemic incidents (those that affect only selected systems) will be addressed next. Examples of this type of incident would be a failed voice gateway router, workgroup server, switch or other system specific infrastructure. The last type of incident to be addressed would be individual or host incidents. This is an incident that only affects one PC on the network, such as a virus, spy ware, or other malicious code.

If an incident meets the criteria as defined by the SANS Institute, it should ultimately be reported to the Incident Response Team. Notification of incidents must be emailed to the appropriate SVCC IT network staff and may be reported by phone or in person as needed as long as email documentation is maintained. Individual team members may respond to the incident as circumstances dictate, if it occurs within their individual area of responsibility. All reasonable and proper troubleshooting methods will be employed to identify, contain, control, any incidents that occur. The team or member(s) will respond to the incident(s) in order of priority as defined above. The actions taken in response to the incident will vary with the type, priority, severity, and magnitude of effect. (See Mitigation Strategies Attachment I 2.1) these actions may be implemented at the discretion of the Incident Response Team member(s) or designated responder.

The strategies outlined in the Incident Response Plan: *Mitigation Strategies* document are a general guideline for timely response to an incident. These guidelines are designed to contain and control deleterious effects on the compromised system and minimize the probability of enterprise contamination. 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.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Incident Response Plan

The next requirement of the plan is that once written guidelines have been established for incident reporting as stated in the IRP and Incident Handling Response Forms (attachment I 2.1) the System Office and Colleges should test the strategies outlined. This testing is to occur as soon as the plan is drafted, and as is necessary, or at least annually prior to June 15. The IRP will be tested along with the DRP testing and evaluated by the Incident Response Team. Once testing is complete, meetings will be held with the Incident Response Team to review all phases of the testing using the IRP strategies evaluation form. (Attachment I 2.1) The college ISO will maintain all testing documentation. Guidelines should be updated accordingly based on the discussion and findings of the team. Questions to be discussed may include:

- Discuss the incident details; what happened?
- Were the written guidelines accessible to the Incident Response Team?
- Did the team perform appropriately? Were procedures followed?
- What additional information was required?
- Were there any actions that inhibited the recovery?
- What would be done differently in a similar incident?
- What additional resources, tools, etc. are needed to assist in future incidents?

Another requirement of the Incident Response Plan is to properly report incidents to the VCCS. 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](#) (see attachment I 2.1) 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

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Incident Response Plan

- 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.

The last requirement of the IRP is that 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. Forensic analysis may be conducted using forensic software or by manually reviewing files and generating reports. The individuals responsible for documentation, and proper completion of all incident response forms are given in: Threat Management: *Incident Handling*, Incident Response forms (attachment I 2.1).