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

Threat Management: *Incident Handling Procedure*

Revision Date	July 1, 2007
Product	Incident Handling
Topic	Threat Detection: <i>Incident Handling</i>
ISO	Will Hamilton, IT Security Analyst, ISO Southside Virginia Community College
Description	<p>The College uses a number of methods to identify and evaluate suspicious activity that may be occurring on the College's computing resources. These include, but are not limited to, Intrusion Detection Systems (IDS), network monitors, LAN packet sniffers, reports from employees, lab technicians, and/or other agencies.</p> <ol style="list-style-type: none">1. Suspicious activity detected by the IDS and LAN packet sniffer that warrants investigation will be entered into the logging database.2. Suspicious activity reported by employees and/or outside entities will utilize the incident reporting forms. <p>SVCC IT staff will utilize SANS incident handling methodology once it has been determined that a system has been compromised.</p> <ol style="list-style-type: none">1. Preparation2. Identification3. Containment4. Eradication5. Recovery6. Lessons learned

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

Threat Management: *Incident Handling Procedure*

	<p>Assumptions:</p> <ol style="list-style-type: none">1. Firewall has security logging turned on.2. Portable sniffer may be connected to any network segment to capture traffic.3. Vulnerability scanners may be used to probe both the internal and external network for potential vulnerabilities.4. All incoming/outgoing email is scanned for viruses. Attachments may be blocked based on filtering rules regardless of whether a virus is detected or not.5. Virus signatures are updated at least once a day on workstations and servers. The email server updates its virus signatures as updates become available for the vendor.
Instructions	<p>Incident handling should follow the steps given below:</p> <ol style="list-style-type: none">1. Complete the Computer Incident Reporting form. (Any IT Staff Member)2. Complete the Incident Contact Information Sheet (Any IT Staff Member)3. Complete Incident Detection Sheet (Network Administrator)4. Complete System Details Sheet (Assigned IT staff member)5. Complete Incident Containment Sheet (Assigned IT staff member)6. Complete Preliminary Investigation Sheet (Assigned IT staff member)7. Complete Incident Eradication Sheet (Assigned IT staff member)7. Report findings to Initiator, IT Director, Security Officer and Network Administrator.8. If necessary, complete the Chain of Custody Form. (IT Network Administrator)9. All incidents will be reviewed by the SVCC Information Technology Security Committee as soon as is practicable.

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

Threat Management: *Incident Handling Procedure*

	Notes:
Location	Attachment I 2.1