

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

##### **Types of IT Security Incidents**

The following is a list of common incidents that may occur. Each type of incident will have a specific set of procedures to follow when an incident occurs. For incidents not listed below, use the procedures in the General Incident type.

- General Incident
- Network Intrusion
- Denial of Service (DoS)
- Virus or other Malicious Code
- Threatening Email
- Illegal Software
- Pornography
- Theft
- Compromised Encryption Keys

##### ***General Incident:***

When a possible incident occurs, always make a quick and best judgment as to whether this is an actual incident. It is best to first assume it is an incident, rather than ignore it and see if it goes away.

When an incident occurs, the most important things to consider are;

- **Safety of personnel.** With IT Security incidents, personnel safety is not a concern except possibly in the case of recovering evidence.
- **Securing Network.** Depending on the type of incident, it may be necessary to disconnect a portion or an entire network from outside access.
- **Preservation of evidence.** In all type of security incidents, preserving evidence is paramount to finding the source of the incident and possible prosecution of individuals responsible for incident. Preservation of evidence may include;

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

freezing of computer resources by unplugging from network (**DO NOT TURN COMPUTER OFF**), saving log files on firewalls, domain controllers and servers, copying log files, email or images of data to CD or DVD.

#### ***Network Intrusions:***

Unauthorized access to any part of the SVCC network should be considered an intrusion to the network. This would include someone who is not a current registered user of the college network or a current SVCC user accessing any part of the network where they are not authorized.

#### **Determining if an Intrusion has taken place:**

It is not always obvious that a break-in has taken place. In some cases it is possible to see the compromise taking place, but in most cases the intrusion has occurred days before it is discovered.

Things to look for when looking for unauthorized access:

- Unusual activity on a computer not being performed by computer operator, such as mouse moving, windows being opened, unusual amount of disk activity.
- Unknown services that are installed.
- Unknown software that has been installed.
- Security log files with large numbers of failed logins, followed by a successful login.

#### **When an intrusion is discovered:**

If a break-in is discovered that is still taking place, remove the computer from the network immediately by unplugging the network cable, **DO NOT TURN MACHINE OFF**. If the break-in is discovered as an unknown service or unknown software, the computer should be removed from the network as soon as possible, because there may be processing running in the background that are not obvious.

Once the computer has been removed from the network, report the break-in to SVCC IT Network Services. IT Network Services will investigate the incident to see if a break-in

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

did occur and recover evidence if available. SVCC IT Network Services will ask you to fill out an IT Security Incident Report Form.

Network Services will work with you to try to determine the source of the break-in and see if the break-in might be more widespread.

Once Network Services has secured the computer and recovered all available evidence, the computer may be returned to service.

After it is determined how the break-in occurred, ALL computers on the network should be checked to see if a similar type of break-in has occurred, and if any damage has been done. Also if possible, it should be determined if any data has been stolen or modified.

If this is the case, all evidence recovered should be forwarded to Buildings and Grounds Security for further investigation and if necessary the appropriate SVCC Management personnel should contact other authorities such as State Police or FBI.

#### ***Denial of Service:***

A denial of service attack is any kind of attack against the network that will disrupt service to users. This attack could be intentional or accidental. The source of the attack could be from outside or from inside the SVCC network. A denial of service attack may affect one or more computers or servers, or the entire network. Generally a denial of service attack is done against a router to cause the loss of service for an entire site, and is usually initiated by one individual, but could be from multiple individuals and multiple sites, which is known as a Distributed Denial Of Service (DDOS) attack.

#### **Router Denial of Service:**

- Report to management that the source of the network problem appears to be a denial of service attack.
- Fill out an IT Security Incident Report Form; make sure times and dates are documented.
- Collect valuable information on source of attack. If the router is configured to cache traffic (ip cache flow), turn on telnet logging and execute the command “sh ip cache flow”. If IP accounting is enabled, execute the command “sh ip accounting”.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## Threat Management: *Incident Handling*

### Incident Response Plan

#### Mitigation Strategies

- Save all logs on the router if possible. Unplug network cable if necessary. (Most of the time during an attack, the CPU is running at 100% and it is impossible to do any task on the router).
- At this point if necessary, reboot the router.
- Before plugging the network cable back in, block the source of the attack using access-lists.
- Review the configuration to see if any changes have been made. A recent backup should be used to compare configurations. If changes have been made or you are unsure, reload configuration from a known good backup.
- The router can now be returned to service by plugging the network cable back into the router. Monitor to see if the router is functioning properly.

#### Server Denial of Service:

- Report to management that the source of the network problem appears to be a denial of service attack.
- Fill out an IT Security Incident Report Form; make sure times and dates are documented.
- Collect valuable information on source of attack. From the command prompt, issue the command “netstat -n > c:\netstat\_*currentdate*.txt”. This will log all current connections to a file. Execute the command “pulist > pulist\_*currentdate*.txt”. This will create a log file of currently running processes. (pulist is not a standard NT tool. This tool should be copied to all servers or used from a tools diskette)
- Disconnect computer or server from the network by unplugging the network cable. **DO NOT TURN OFF THE COMPUTER.**
- Open Event Viewer and save Application, Security and System log files to text files.
- Review the list of installed services and the log file of running processes. If any processes or services are running that are not normal, you need to find out where

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## Threat Management: *Incident Handling*

### Incident Response Plan

#### Mitigation Strategies

the executables are located. For services, you can view the property of a service and it will show the executable. For a process that is only running in memory, you may have to search the hard drive for the executable file. Once the executable file has been located, view the security properties of this file and find out who the owner is. This will tell you what account was used to copy the file to the server. If the owner is the administrator account or a domain administrator account, all administrator account passwords must be changed.

- If a service was installed, delete the service using the resource kit utility “delsrv *servicename*”.
- If a process was running in memory, the executable was either put in a startup group or most likely into the registry. Delete the executable files from the hard drive along with any .dll or configuration files for that process. Open the registry and go to  
\\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run and  
\\HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Runonce to see if there are any unusual programs that will run at startup.
- Before putting the computer or server back on the network, perform a full virus scan with most recent virus definitions.
- Computer or server may be returned to network only after the above steps have been completed and server rebooted.

#### ***Virus or other Malicious Code:***

All SVCC workstations and servers are running Symantec or Norman virus software. Since all file servers and mail servers are configured to automatically update the virus definitions, most virus' are stopped before they can do any damage or propagate to other computers. However, malicious code could be released and infect a computer before an update is released from the virus software vendor. By monitoring news agencies and virus alert websites, we can see when a new virus has been discovered, and prepare to update the virus software as soon as an update is released or take measures to block the virus from entering the network.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

If a virus or other malicious code does enter the SVCC network, the following steps should be taken to stop them from spreading and disrupting the network.

- If possible, update the virus software on the infected workstation or server.
- Isolate infected computer by removing it from the network.
- Try to determine if the infection is localized or spread to other computers.
- If the infection is to a single computer, scan the computer and clean the infected files. If the files cannot be cleaned, they should be deleted.
- If the infection is on many computers, it may be necessary to disconnect the entire subnet from the network. This can be done by shutting down the VLAN on the router.
- Once all the infected computers are isolated, scan and clean them.
- While computers are being cleaned, try to determine the source of the infection.
- If the infection was caused because a computer has not been updated with Microsoft patches, update the computer while it is offline using a CD or floppy disk.
- If the infection was caused by an email that was opened, the email server in question needs to be investigated to determine the cause of the issue.
- After the infected computers have been cleaned and the source of the virus has been found and stopped, the computers can be returned back to the network.

#### ***Threatening Email:***

Occasionally SVCC receives complaints about either a threatening email being sent from the SVCC network, or a user receives a threatening email from outside the college. When tracking a threatening email, the header information from the original email, is the most valuable piece of information for tracking an email. The header information needs to be from the original email and not from a forwarded email, since the header information is changed when the email is forwarded. All threatening emails and the consequences associated therewith will be addressed by SVCC President's staff.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## Threat Management: *Incident Handling*

### Incident Response Plan

#### Mitigation Strategies

##### **Threatening Email Sent From Inside the College:**

When notified that a threatening email has been received by someone outside the college and they believe the email originated inside the college, you must first determine if the email was sent from the college email system or from a pop account such as Hotmail, \ Yahoo, AOL or Netscape Mail. If a user is using Outlook Express as their mail client to the Microsoft Exchange server, the header information will resemble a pop mail client's header.

By examining the header of the email, you should be able to identify the senders IP address. In Figure 1, a message was sent from Exchange to a Yahoo account. In Figure 2, an email was sent from a Yahoo account to an email account on adelphia.net. The header information contains a limited amount of useful information. The "**Return-Path**" is usually faked, but if the message was sent from the Exchange server, the email address in the "**Return-Path**" may be accurate. The most important lines are the "**Received: from**", "**Message-ID**" and "**Date**:"

In Figure 1, the email was sent from Novamail, with the IP address of 164.106.14.137. Since the email was sent from an Exchange mail server, the IP address in the "**Received: from**" line is the IP address of the mail server, not the IP address of the senders machine. The "**Message-ID**:" line contains the sender's mail server, Novamail3.nv.cc.va.us.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## Threat Management: *Incident Handling*

### Incident Response Plan

#### Mitigation Strategies

```
X-Apparently-To: testperson@yahoo.com via 66.218.93.145; Wed, 02 Jun 2004 12:09:30 -0700
Return-Path: <tperson@nvcc.edu>
Received: from 164.106.14.137 (EHLO novamail.nv.cc.va.us) (164.106.14.137) by
mta272.mail.scd.yahoo.com with SMTP; Wed, 02 Jun 2004 12:09:30 -0700
Received: by novamail.nv.cc.va.us with Internet Mail Service (5.5.2656.59) id <KG6JK3HG>; Wed, 2
Jun 2004 15:09:29 -0400
Message-ID: <9B6747DA260EE8418C6EF44FA5E29D1509AEB8@novamail3.nv.cc.va.us>
From: "Test Person" <tperson@nvcc.edu> Add to Address Book
To: "'testperson@yahoo.com'" <testperson@yahoo.com>
Subject: Hello Test Here
Date: Wed, 2 Jun 2004 15:09:19 -0400
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.2656.59)
Content-Type: multipart/alternative; boundary="----_=_NextPart_001_01C448D5.1AF78700"
Content-Length: 922
```

**Figure 1 – Header from email sent from Exchange server inside the network.**

In Figure 2, the email was sent from a Yahoo account from a computer inside the network. Notice in the “**Received:** from” line, the IP address of the sender, 164.106.68.28, is the senders IP address.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

**Return-Path:** <testuser2000@yahoo.com>  
**Received:** from web13526.mail.yahoo.com ([216.136.174.216]) by mta2.adelphia.net (InterMail vM.5.01.06.08 201-253-122-130-108-20031117) with SMTP id <20040603022521.JJSA1089.mta2.adelphia.net@web13526.mail.yahoo.com> for <testsend@adelphia.net>; Wed, 2 Jun 2004 22:25:21 -0400  
**Message-ID:** <20040603022521.49369.qmail@web13526.mail.yahoo.com>  
**Received:** from [164.106.68.28] by web13526.mail.yahoo.com via HTTP; Wed, 02 Jun 2004 19:25:21 PDT  
**Date:** Wed, 2 Jun 2004 19:25:21 -0700 (PDT)  
**From:** Test User <testuser2000@yahoo.com>  
**Subject:** Test Message from Yahoo  
**To:** testsend@adelphia.net  
**MIME-Version:** 1.0  
**Content-Type:** text

**Figure 2 - Header from email sent from a Yahoo account from inside the network.**

**In Figure 2, the email was sent from a Yahoo account from a computer inside the network. Notice in the “Received: from” line, the IP address of the sender, 164.106.68.28, is the senders IP address.**

If by examining the headers, you determine that the email was sent from an inside Exchange account, follow the steps below to locate the user;

- Fill out an IT Security Incident Report Form.
- Record date and time the email was sent (take this information from the email header).
- Record the information from the “**Return-Path:**” line. (If the email was sent from an Outlook client or from Outlook Web Access, this information should be correct. If the email was sent from an Outlook Express client, the email address in the “**Return-Path**” line may be incorrect.
- Record the “**Message-ID**” information. If tracking logs are enabled on the Exchange server, the “**Message-ID**” line can be used to track the message on the mail server.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **Threat Management: *Incident Handling***

### **Incident Response Plan**

#### **Mitigation Strategies**

If by examining the headers, you determine that the email was sent from a pop mail client, follow the steps below;

- Fill out an IT Security Incident Report Form.
- Record date and time the email was sent (take this information from the email header).
- Record the information from both “Received: from” lines. The information in the first “Received: from” line is the mail server that received the email (usually of no help). The information in the second “Received: from” line, contains the IP address of the computer that sent the email.
- The IP address of the computer that sent the email is a public IP address. In instances where Network Address Translation (NAT) is used on the firewall, the public IP address will have to be translated to the local private IP address used on the firewall.
- To translate the public IP to the correct private IP, you will need to open the firewall logs. Using the date and time from the email header, go to the firewall logs, open the log file dated the same as the date in the email header.
- Do a search for the public IP address in the firewall log. Search until you find the public IP address at the correct date and time that was in the email header. (The time may vary slightly) When the public IP address is found, it will show the corresponding private IP address. In the example below, the public IP address, 164.106.14.130 is assigned to the private IP address 10.30.9.254.

```
2003-06-03 00:01:08  News.Info  10.30.x.x  Jun 03 2003 00:00:13: %PIX-6-302013: Built outbound TCP connection 119047622 for outside:192.175.48.1/53 (192.175.48.1/53) to inside:10.30.9.254/2409 (164.106.14.130/2409)
```

**Figure 3 – Firewall log example**

---

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

---

**Threat Management: *Incident Handling***

**Incident Response Plan**

**Mitigation Strategies**

- Once you have the private IP address, you can find out what computer the IP address belongs to by executing the command “nbtstat -a 10.30.9.254” from a command prompt on a Windows 2000 and Windows XP computer on the same network.
- Another point to consider is that Dynamic Host Control Protocol (DHCP) may be used internally, so the private IP address that is found in the firewall log, may not match the computer, if the email is not recent.

***Illegal Software:***

- Verify with the end user and media processing that the software is in fact not licensed.
- Fill out the IT Security Incident Report form and forward to the IT Security Officer.
- The IT Network Administrator will verify if licensing needs to be procured or that the software be removed and will notify the campus VP of IT and ISO.

***Pornography:***

- Fill out the IT Security Incident Report form and forward to the IT Security Officer and IT Network Services.
- The IT Staff/ Network Administrators will verify that the offensive material has been removed and will notify the campus Provost and ISO.

***Theft of Computer Equipment:***

- Notify Buildings and Grounds security and the Fixed Assets Manager.
- Fill out the IT Security Incident Report form and forward to the IT Security Officer.
- IT Security Officer will perform any IT related investigation required; the physical and legal aspects of such an incident will be handled by the Fixed Assets Manager or designated member of SVCC management.

---

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

---

**Threat Management: *Incident Handling***

**Incident Response Plan**

**Mitigation Strategies**

***Encryption Keys are compromised:***

- Terminate connection to remote host; Contact IT Network Services immediately.
- Fill out the IT Security Incident Report Form and forward it to IT Network Services and SVCC ISO.

***Incident Response Quick Check List:***

	<b>Mission Critical</b>	<b>Global</b>	<b>Systemic</b>	<b>Host</b>
<b>Incident description:</b>				
Denial of Service	3, 4	3, 4	3, 4	3, 4, 5
Malicious Code	2, 3, 4, 5	2, 3, 4, 5	2, 3, 4, 5	2, 4, 5
Unauthorized Access	3, 4, 5, 6	3, 4, 5, 6	3, 4, 5, 6	3, 4, 5, 6
Misuse of System	2, 3, 4, 6	2, 3, 4, 6	2, 3, 4, 6	2, 3, 4, 6
Threat/Harassment via electronic medium	3, 4, 6	3, 4, 6	3, 4, 6	3, 4, 6
Other (describe)				

**\*Response:**

1. No action taken
2. Restore data from backup
3. Examine system log files
4. Disconnect from network or shutdown system
5. Update virus/spyware software and scan computer
6. Physically secure device
7. Other (describe) \_\_\_\_\_

***\*All incidents must be reported to the proper personnel.***