

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **IT Contingency Planning** *Continuity of Operations Planning (COOP)*

### College Network Contingency Guide

Scheduled or unscheduled outages of information technology(IT) services and infrastructure on a community college campus or at the System Office can and do impact the IT service delivery at other campuses, community colleges, and for those customers who may be accessing the services from an off campus location. An outage may have a short duration; however there are situations that could cause an outage to last for an extended time period. The primary concern is how best to communicate information regarding the outage in a way that permits those who are dependent on the services to receive current and accurate information for their decision making. This document outlines planning activities and related actions to be taken to ensure consistent communications in the event of a scheduled or unscheduled outage that impacts critical IT services.

This document describes actions to be taken by College and System Office personnel in the event of an unexpected or anticipated major outage or interruption of IT services at a college such as the failure of a primary network circuit, loss of the Internet connection, or extensive damage to the physical facilities. Such an outage could be caused by human error or an unexpected natural disaster that would force a closure and/or put the operations at risk due to potential power outages. Similarly, if any VCCS entity experiences or anticipates any type of major outage or interruption in IT services that will impact the VCCS Intranet or delivery of services to colleges then this Plan is to be invoked.

All VCCS colleges have an internal network infrastructure as well as a high speed connection to the VCCS primary network for the delivery of key IT services including voice services. The System Office also provides system wide access to all enterprise applications and services using the same primary network. Since an unexpected outage to network services whether on the campus or on the backbone could adversely impact the performance or service delivery at or to other VCCS locations. Therefore each college and the System Office must be prepared not only to maintain the local operations, but also work in a coordinated fashion with the other colleges and the System Office to maintain the IT service delivery for VCCS.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **IT Contingency Planning** *Continuity of Operations Planning (COOP)*

### College Network Contingency Guide

#### Preparation

Colleges and the System Office should prepare in advance for system, network and infrastructure failures and interruptions by taking the following actions:

1. All entities should have a current disaster preparedness and recovery plan. This plan should identify key components, key personnel, and actions to be taken in various eventualities. In particular, it should address backup and recovery, and procedures to be followed in the event of major storms or power outages. A contact procedure should be developed and documented, so that Campus security, facilities, and both the college and Information Technology Services (ITS) at the System Office personnel can contact each other and can be contacted by the college senior administrative staff.
2. Colleges and the System Office should be prepared to restore their web presence at an alternate location to ensure that students, faculty, staff and other stakeholders are kept informed during a disaster or other circumstance that causes primary IT services and applications to be unavailable. If an entity does not have the capacity to restore their entire web presence quickly, a single web page with announcements and links to enterprise resources should be made available in the interim. Entities who maintain their own DNS servers should also take steps to ensure that DNS records can be changed quickly, even if their primary data center is destroyed or otherwise unavailable. The ITS Enterprise Services at the System Office will work with colleges to provide guidance and assistance where necessary.
3. The local network should be made as resilient as possible utilizing UPS and generator resources whenever possible. These units should be sized to cover at least the brief interruptions that may occur during a normal summer thunderstorm. The servers should be configured to perform a normal, controlled, shut down should the power outage extend beyond the capacity of the UPS. At a minimum, the primary network edge equipment, currently the edge router, firewall and voice gateway should be protected by an UPS with a two to four hour capability.

---

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

---

**IT Contingency Planning**  
*Continuity of Operations Planning (COOP)*

College Network Contingency Guide

4. All entities should provide ITS Client Services at the System Office with a list of key contacts, including home phone numbers, pager numbers, and cell phone numbers in case problems occur during off hours which require the System Office ITS Client Services to contact the appropriate personnel. These numbers can either be the direct numbers of the personnel themselves or the numbers for an Office who in turn should be able to notify the appropriate staff.
5. ITS Client Services to contact the appropriate personnel. These numbers can either be the direct numbers of the personnel themselves or the numbers for an Office who in turn should be able to notify the appropriate staff.
6. All entities should implement the standard automated problem management software so incidents can be tracked and managed by the System Office ITS Client Services.
7. Entities connected to the MPLS Backbone side of the VCCS primary network should have at a minimum two individuals with access to the network provider customer care center for entering trouble tickets.

**PRE- CLOSING ACTIONS**

Should an outage be anticipated due to a predicted major storm, or any other reason, the appropriate personnel should contact the System Office ITS Client Services, informing them of the entities plans. The entity could make one of two choices:

1. Close as appropriate, but allow the local network and primary network equipment to stay on line. In this case, the System Office ITS personnel will monitor the status of the entities primary network equipment.
2. In coordination with the System Office ITS personnel, take down the entities network and primary network equipment and establish the alternative web site presence.

Should the outage occur unexpectedly, the appropriate College personnel should contact the System Office ITS Client Services, if possible, to inform them of the situation and to coordinate planning to restore network services.

---

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

---

**IT Contingency Planning**  
*Continuity of Operations Planning (COOP)*

College Network Contingency Guide

**DURING OUTAGE OR CLOSING**

During the time the entity is closed, the safety of personnel is the primary concern. Nothing should be done that would put any personnel at any significant risk. However key personnel should remain in contact with the System Office ITS Client Services. As soon as the entity can predict an opening time or the time the services will be restored, the System Office ITS Client Services should be informed.

**RE-ESTABLISHING THE PRIMARY NETWORK CONNECTION**

Once it is safe to return to the location; and power, telephone, and other utilities have been reestablished, or when it is otherwise feasible to restore the network services; network and other information technology personnel working with the System Office ITS staff should restore the network to a normal operational status.

**POST MORTEM**

Once the entity is back in normal operations, the key people responsible for the shutdown activities and the restoration of services should analyze the actions taken. They should also document in the problem management incident what happened and make any necessary changes to their disaster recovery plan. Comments from the System Office ITS staff and from on and off campus users should be included in developing the post mortem report.

**FAILSAFE PROCEDURES**

In the event an entity experiences or anticipates any type of outage or interruption of IT services that is adversely impacting the VCCS Intranet or IT services being provided to other colleges, the following Failsafe Procedures will be invoked.

- 1) Should an entity detect that one of its circuits is unavailable; the appropriate IT staff should notify the System Office ITS Client Services either via email, problem management software or telephone. The appropriate IT staff should also open a ticket with the network provider.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

## **IT Contingency Planning** *Continuity of Operations Planning (COOP)*

### College Network Contingency Guide

- a) If the location is connected via a T1 or DS3 circuit, the appropriate IT staff can open a trouble ticket using the network provider customer care center
- b) If the location is connected via Ethernet, the appropriate IT staff can open a trouble ticket by calling the current service provider.

staff must be prepared to answer the following questions that will be asked by the network provider technician:

- Type of Data Service reported
- Circuit ID # and Site Address
- Description of Trouble
- Advise if customer provided equipment has been checked (ie. Power, Error Indications, cabling, A/C)
- Advise if intrusive testing can be performed
- Site Access Information: Site Access Times and Site Contact Information

To provide the quickest resolution, staff must provide an onsite Contact name and phone number in the case that a network provider Technician has to come to the site to resolve the issue. Failure to do so may delay the restoration of services.

The System Office ITS Network staff must be contacted if the trouble ticket has to be escalated.

- 2) Should the System Office ITS Staff detect a campus circuit is down, the System Office ITS Network staff will try to contact the appropriate IT Staff to confirm or notify them about the outage. ITS Network Staff will notify ITS Client Services and open a trouble ticket with network provider to start the process of resolving the issue.
  - a) In the event that an entities staff can not be reached, ITS Network staff will open a trouble ticket but will not allow intrusive testing to be performed without confirmation from the appropriate IT staff.
  - b) The entities onsite staff must be contacted before network provider technicians can be dispatched for onsite testing if that is deemed necessary.
- 3) The System Office ITS Client Services will send out a broadcast email notifying everyone of the outage
  - a) When required, the System Office ITS Client Services will also take additional steps to notify users, such as posting a notice on MYVCCS and Blackboard web pages.

---

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

---

**IT Contingency Planning**  
*Continuity of Operations Planning (COOP)*

College Network Contingency Guide

- 4) In the event a server is creating system wide problems such as a compromised server attempting to infect other servers or network devices. The System Office ITS Network staff will attempt to contact the appropriate point of contact for the rogue site in an effort to get the appropriate staff to correct the situation. In the event System Office ITS Network staff cannot contact the appropriate staff to get the situation resolved at the local level, the System Office ITS Network staff, as deemed necessary to protect other entities and networks and with approval from the CISO or a Director of ITS at the System Office, will quarantine the infected server so that normal operations may be restored to the rest of the network.
- 5) When the problem has been resolved, the System Office ITS Network staff will work with the appropriate staff to expeditiously reestablish connectivity for the site in question.

**CONCLUSION**

It is imperative that the network and related IT services remain available at all times serving as many customers as is possible. The standard outlined in this document provides the System with a means of ensuring that continuous uninterrupted VCCS primary network access and support is available to the majority of the VCCS customers under the most adverse conditions. Working together we can minimize the impact of a failure so that it affects as few customers as possible