

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

IT Contingency Planning
Continuity of Operations Planning (COOP)

Recovery Strategies for Mission Critical Processes

Continuity of Operations Planning (COOP) includes developing plans necessary to provide continuity of essential SVCC systems and data in accordance with [COV ITRM 501-01](#).

This Standard addresses the development, implementation, exercise, and maintenance of the Continuity of Operations Plans as it relates to IT systems and data.

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and maximum allowable outage times identified in the BIA and Risk Assessment processes. The SVCC mission critical business processes identified during the BIA, and recovery strategies for each are as follows:

Academic and Student Affairs:

Faculty Evaluations:	Process ID: ASA-07-4
Application:	MS Office 2003, Dell PC
Criticality:	2
Acceptable Downtime:	Dependant on external deadlines
Recovery Strategy:	RS-07-1

Faculty Pay: Overloads	Process ID: ASA-07-5
Application:	MS Office 2003, Dell PC
Criticality:	2
Acceptable Downtime:	Dependant on external deadlines
Recovery Strategy:	RS-07-1

Faculty Hiring:	Process ID: ASA-07-7
Application:	MS Office 2003, Dell PC
Criticality:	2
Acceptable Downtime:	Dependant on external deadlines
Recovery Strategy:	RS-07-1

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

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

Recovery Strategies for Mission Critical Processes

Administrative and Financial Services:

Payroll Accounts: HR-07-1
Application: CIPPS, CARS, PMIS, FRS, PeopleSoft,
Oracle 10.G, Dell PC
Criticality: 1
Acceptable downtime: 1 hour
Recovery Strategy: RS-07-1

Manage leave, benefits: HR-07-2
Application: CIPPS, CARS, PMIS, FRS, PeopleSoft,
Oracle 10.G, Dell PC
Criticality: 2
Acceptable downtime: 1 day
Recovery Strategy: RS-07-1

Maintain personnel records: HR-07-3
Application: CIPPS, CARS, PMIS, FRS, PeopleSoft,
Oracle 10.G, Dell PC
Criticality: 2
Acceptable downtime: 1 day
Recovery Strategy: RS-07-1

Reporting, internal/external: HR-07-5
Application: CIPPS, excel, Dell PC
Criticality: 2
Acceptable downtime: 1 day
Recovery Strategy: RS-07-1

Record employee hours: HR-07-6
Application: CIPPS, excel, Dell PC
Criticality: 2
Acceptable downtime: 1 day
Recovery Strategy: RS-07-1

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

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

Recovery Strategies for Mission Critical Processes

Hiring, applicant records:	HR-07-4
Application:	RMS, PMIS excel, Dell PC
Criticality:	2
Acceptable downtime:	1 day
Recovery Strategy:	RS-07-1
Accounts receivable:	BO-07-1
Application:	PeopleSoft 8.9, Oracle 10.G, Dell PC
Criticality:	2
Acceptable downtime:	1 day
Recovery Strategy:	RS-07-1
Accounts payable:	BO-07-2
Application:	FRS, Dell PC
Criticality:	2
Acceptable downtime:	1 day
Recovery Strategy:	RS-07-1
Building Security:	SEC-07-1
Application:	Proprietary system, console and controller
Criticality:	1
Acceptable downtime:	2 days
Recovery Strategy:	RS-07-1
Fire Prevention:	SEC-07-3
Application:	Proprietary system, console and controller
Criticality:	1
Acceptable downtime:	1 day
Recovery Strategy:	RS-07-1
Accounts receivable:	BS-07-1
Application:	FRS, Dell PC
Criticality:	2
Acceptable downtime:	1 week
Recovery Strategy:	RS-07-1

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

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

Recovery Strategies for Mission Critical Processes

Accounts payable:	BS-07-2
Application:	FRS, Dell PC
Criticality:	2
Acceptable downtime:	1 week
Recovery Strategy:	RS-07-1

Admissions & Records, Institutional Research:

Transcript processing:	AR&IR-07-3
Application:	PeopleSoft 8.9, Oracle 10.G, Dell PC
Criticality:	2
Acceptable downtime:	3 days
Recovery Strategy:	RS-07-1

Monitoring student records:	AR&IR-07-4
Application:	PeopleSoft 8.9, Oracle 10.G, Dell PC
Criticality:	2
Acceptable downtime:	1 day
Recovery Strategy:	RS-07-1

Manage student accounts:	FA-07-1
Application:	PeopleSoft 8.9, Oracle 10.G, Dell PC
Criticality:	2
Acceptable downtime:	1 week
Recovery Strategy:	RS-07-1

Disburse funds:	FA-07-2
Application:	PeopleSoft 8.9, Oracle 10.G, Dell PC
Criticality:	1
Acceptable downtime:	1 week
Recovery Strategy:	RS-07-1

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

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

Recovery Strategies for Mission Critical Processes

Institutional Advancement:

Maintain donor records:	IA-07-2
Application:	MS office 2003 Dell PC
Criticality:	2
Acceptable downtime:	3 days
Recovery Strategy:	RS-07-1

Student Services:

Billing:	SS-07-10
Application:	PeopleSoft 8.9, Oracle 10.G Dell PC
Criticality:	1
Acceptable downtime:	4 hours
Recovery Strategy:	RS-07-1

Workforce Development:

Maintain student records:	WFD-07-2
Application:	PeopleSoft 8.9, SIS, Dell PC
Criticality:	2
Acceptable downtime:	2 weeks
Recovery Strategy:	RS-07-1

Registering students:	WFD-07-1
Application:	MS office 2003, PeopleSoft 8.9, Dell PC
Criticality:	2
Acceptable downtime:	2 weeks
Recovery Strategy:	RS-07-1

Billing:	WFD-07-13
Application:	PeopleSoft 8.9, EVa Dell PC
Criticality:	2
Acceptable downtime:	Dependant on external deadlines
Recovery Strategy:	RS-07-1

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

IT Contingency Planning
Continuity of Operations Planning (COOP)

Recovery Strategies for Mission Critical Processes

Receive payments:	WFD-07-6
Application:	MS office, PeopleSoft 8.9, SIS, Dell PC
Criticality:	2
Acceptable downtime:	Dependant on external deadlines
Recovery Strategy:	RS-07-1

Work Keys testing:	WFD-07-8
Application:	MS office, Database, scanner, Dell PC
Criticality:	2
Acceptable downtime:	2 weeks
Recovery Strategy:	RS-07-1

Instructor records:	WFD-07-9
Application:	MS office, PeopleSoft 8.9, SIS, Dell PC
Criticality:	2
Acceptable downtime:	2 weeks
Recovery Strategy:	RS-07-1

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

IT Contingency Planning
Continuity of Operations Planning (COOP)

Recovery Strategies for Mission Critical Processes

Recovery Strategies: RS-07-1

1. Contact network services stating the nature of the problem. Users may contact network services via telephone, email (required), or face-to-face.
2. Networks services personnel will determine the nature of the problem.
 - LAN based problems: To be repaired by network services staff within the acceptable downtime window for the application or process.
 - WAN based problems: Network services will work with the SVCC utility, ISP's, TelCo, and any other entity deemed necessary to facilitate restoration of services within the acceptable downtime window for the application or process.
3. Develop alternate manual procedures for mission critical business processes. The manual procedures as promulgated by the system and/or activity owners are given in the IT Contingency Planning: *COOP, manual procedures for mission critical business functions* document, Attachment C 1.1.
4. Problems with equipment or systems under third party maintenance contracts:
Contact the appropriate vendor:
Reference: IT Contingency Planning: *Disaster Recovery Planning, emergency telephone numbers, and vendor list* documents, Attachment C 2.3. Also the Personnel Security: *Access Determination and Control, authorized access personnel* document, Attachment H 1.1.

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

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

Recovery Strategies for Mission Critical Processes

5. For any situation that may cause data that is subject to FERPA regulations to be compromised, the following actions may be taken:
- Determine and document the specific data that was compromised.
 - Contact SVCC administration, and the college ISO.
 - SVCC administration will contact the VCCS for guidance.
 - The following website may be useful in determining appropriate actions to be taken:
www.ed.gov/policy/gen/guide/fpco.index.html

Or the agency may be contacted at the following address:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-5920

Network Infrastructure:

Cisco equipment covered under SmartNet:

The SVCC network infrastructure equipment is covered by the Cisco SmartNet 8 x 5 x NBD. This contract covers any hardware problem and parts with the following equipment: (see *SVCC IT Business Environment* documents maintained by IT Network services at each campus).

In an event of a hardware failure of any of the following equipment, the following procedure is done:

If the Internet is accessible go to
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> and follow the directions or call (800) 553-2447 if Internet access is unavailable.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

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

Recovery Strategies for Mission Critical Processes

Opening a Case

The online TAC Case Open Tool (www.cisco.com/tac/caseopen) is the fastest way to open **P3 and P4** (priority 3 and 4) cases. After you describe your situation, the TAC Case Open Tool recommends resources for an immediate solution. If your issue is not resolved via these automatic solutions, your case will be assigned to a Cisco TAC engineer.

For **P1 or P2** (priority 1 and 2) cases (when the production network is down or severely degraded) or if you do not have Internet access, contact the Cisco TAC via telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case via telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, please visit:

http://www.cisco.com/en/US/support/tsd_contact_technical_support.html

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

- **Priority 1 (P1)**—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
- **Priority 2 (P2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- **Priority 3 (P3)**—Operational performance of your network is impaired while most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

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

IT Contingency Planning
Continuity of Operations Planning (COOP)

Recovery Strategies for Mission Critical Processes

- **Priority 4 (P4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

The SVCC CCO contract information is maintained by the IT Network Administrators.

- Contact the Cisco Sales Representative at Dimension Data, Cynthia Reason (919) 791-1088; cynthia.reason@us.didata.com or the DISYS Sales Representative for Cisco Brian Dibble 757-903-7170; brian.dibble@disys.com and place order for replacement Cisco equipment. Cisco will usually overnight equipment damaged in a catastrophic event.
- DiData or DISYS may supply network technicians (at additional cost) who will assist in the installation and configuration of Cisco network infrastructure equipment.
- The SVCC IT Network Administrators maintain a backup configuration of every Cisco device on the SVCC network.

Cisco Equipment not covered under SmartNet:

Some Cisco switches, Cisco IP phones, and Cisco Wireless Access Points are not covered under the Cisco SmartNet agreement. The SVCC IT Network staff maintains spare units of each type of equipment to replace units that have failed.

Replacement of Cisco Equipment that is damaged or destroyed by fire, flood, hurricane, earthquake, or due to theft:

The Cisco SmartNet maintenance agreement does not cover equipment stolen or destroyed due to fire, flood, hurricane, earthquake, or by any other external force. In order to recover from such a catastrophic event, SVCC IT Network staff would perform the following steps:

- Assess the damage and take inventory of what needs to be replaced.
- Determine if the building and computer room or closet is still usable.
- Clear out the destroyed equipment and prepare location for replacement equipment.
- Call the COV Department of Treasury and contact the Risk Management officer

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

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

Recovery Strategies for Mission Critical Processes

- to submit insurance claim. Ph (804) 786-3152 (select option 1).
- Contact the Cisco Sales Representative at Dimension Data, Cynthia (919) 791-1088; cynthia.reason@us.didata.com or the DISYS Sales Representative for Cisco Brian Dibble 757-903-7170; brian.dibble@disys.com and place order for replacement Cisco equipment. Cisco will usually overnight equipment damaged in a catastrophic event.
 - DiData or DISYS may supply network technicians (at additional cost) who will assist in the installation and configuration of Cisco network infrastructure equipment.
 - The SVCC IT Network Administrators maintain a backup configuration of every Cisco device on the SVCC network.

System servers and workstations:

Devices covered under Maintenance Service Agreement:

(SVCC devices with four year onsite parts and labor maintenance service contract listed with the manufacturer). When the maintenance service contract expires, the device will be replaced with a new one and a new four year maintenance service contract (as practicable and as budgeted for).

When an SVCC server or workstation fails due to a hardware problem, the SVCC IT network staff will call the appropriate manufacturer; provide the devices serial number to the Technical Support technician. The replacement part will be delivered the next business day. The manufacturer service technician will be onsite the next business day to install the replacement part. In most cases, an SVCC IT network staff member will volunteer to install the replacement part.

Replacement of servers or workstations not covered by maintenance or that are damaged or destroyed by fire, flood, hurricane, earthquake, or due to theft:

The maintenance agreements and do not cover equipment stolen or destroyed due to fire, flood, hurricane, earthquake, or by any other external force. In order to recover from such a catastrophic event, the SVCC IT staff would perform the following steps:

- Assess the damage and take inventory of what needs to be replaced.
- Determine if the building and computer room or closet is still usable.

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

IT Contingency Planning
Continuity of Operations Planning (COOP)

Recovery Strategies for Mission Critical Processes

- Clear out the destroyed equipment and prepare location for replacement equipment.
- Call the COV Department of Treasury and contact the Risk Management officer to submit insurance claim. Ph (804) 786-3152 (select option 1).
- Contact the proper vendors and place an order to replace affected devices.

The SVCC IT Network Administrator will install the server networking operating system and restore the server configuration, applications, and data files from the server backup tapes.