
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Introduction

The following is a general guide for the implementation of the SVCC IT Contingency Planning: *Disaster Recovery Plan*. This guide is to be used as a reference in order to respond to an IT Disaster in a timely fashion. Given below is the order of operations necessary to identify the various components, and perform the various functions, of the SVCC Disaster Recovery Plan. Information such as locations of specific plan documents, management structure, employee roles and responsibilities, and prioritization for reestablishment of services will be given.

This IT Disaster Recovery Plan was developed in conjunction with the College's *Crisis Management Plan* and the *SVCC COOP Plan* to allow a rapid and organized response to the full or partial destruction of the College's information technology capabilities. Resources that could potentially be destroyed or impaired include the following: information, equipment, and physical space housing the equipment, software, and personnel. The importance of planning for the eventuality of such losses is vital to the amount of damage, decreasing the length of outages, and lowering the cost of recovery.

Assumptions

This plan was developed based on the following assumptions:

1. One of the sites will survive the disaster.
2. Backup media and documentation will be secure at the surviving site.
3. Personnel can be made available to implement the Disaster Recovery Plan.
4. In the event of total or partial loss of the College's computer services personnel, assistance will be available from the Virginia Community College System (VCCS) personnel to implement the Disaster Recovery Plan.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

5. In case of widespread regional disruption, access to emergency resources and personnel may be severely limited.

When an IT Disaster is recognized

In the event of an IT disaster or as notified following a business-wide disaster, the IT Disaster Planning Coordinator Mr. Will Hamilton will initiate IT disaster recovery procedures. If Mr. Hamilton is not available the order of responsibility for initiating IT disaster recovery procedures is as follows: Mr. Jack Ancell, Mr. Peter Hunt or any other SVCC senior management as may be necessary. The IT disaster planning coordinator or substitute will secure a copy of the current disaster recovery plan. Current copies of the disaster recovery plan reside in the Workforce Development Center, Daniel Campus, Keysville, VA and the Workforce Development Center, Christanna Campus, Alberta, VA. The IT disaster planning coordinator or substitute will perform a quick analysis of the situation and notify administrative staff at the VCCS and/or individual college as applicable, and computer customers and will call and place into service the appropriate IT disaster teams (description of possible IT disaster teams listed below). The IT disaster planning coordinator or substitute will work with other disaster recovery teams to facilitate communication and coordination of efforts.

The Planning Coordinator will perform the following duties:

1. Serve as the primary contact and coordinate the recovery effort.
2. Contact all support personnel involved in the recovery effort.
3. Provide all support personnel with a copy of the recovery plan.
4. Contact the Emergency Management Team as soon as possible.
5. Maintain the Disaster Recovery Plan.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Emergency Management Team: (Attachment C 2.3)

- IT Disaster Planning Coordinator
- Network Administrator
- Information Security Officer
- College President
- College Provost
- Buildings and Grounds Supervisor
- Administrative, Financial, and Facilities Management Department Head

The Emergency Management Team will make decisions based on information received from the Technical Support Team and other Emergency or Security personnel.

The Emergency Management Team will be responsible for the following:

1. Establishing a command and control center. The Conference Room (at either Campus) is designated as the command and control center. In the event that the primary on-site command and control center is rendered unusable, the alternate on-site location is the Library. If all on-site facilities are rendered unusable, the command center will be located on the surviving Campus.
2. Contacting and briefing the following management on the status of the contingency:
 - a. Deans of Instruction
 - b. Director of Student Services
 - c. Vice President of finance
3. Notifying the appropriate individuals and vendors per Section C 2, Emergency Telephone Numbers List, Emergency Teams, documents (Attachment C 2.3)
4. Prioritization of critical applications.

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

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Emergency Procedures

5. Make decisions on recovery steps using the Disaster Recovery Plan and any other information available to the Emergency Management Team.
6. Appoint replacement staff if required.
7. Establish a timetable for restoring normal operations.
8. Implement emergency procurement procedures consistent with the Department of General Services' Agency Procurement and Surplus Property Manual.

Technical Support Team: (Attachment C 2.3)

- Network Administrator
- Blackboard Administrator
- PeopleSoft Administrator
- Information Security Officer
- Network Administrator
- Installation and Repair Technician
- Essential Buildings and Grounds Personnel
- Any other personnel deemed necessary for this team

The Technical Support Team will have the following responsibilities:

1. Ascertain when safe entry into is possible to retrieve backup media.
2. Contact all vendors and meet with them on site to assess the damage.
3. Within 24 hours, provide the Emergency management team with an assessment of the damage sustained by IT resources. The briefing will include the following:

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

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Emergency Procedures

- a. Identification of the damaged resources
 - b. Identification of resources that may be salvageable
 - c. Review of critical applications
 - d. Feasibility of restoring services on an interim basis for critical applications
 - e. Status of vendor requests
 - f. Requirements of site security
 - g. Restoration of all backup media
 - h. Restoration of LAN/WAN communications
 - i. Salvage usable equipment, software, and documentation
 - h. Restoration of all backup media
 - j. Procurement of replacement equipment, software, and services
 - k. Reestablish communication with and access to VCCS Network
4. Schedule, coordinate, and communicate with other disaster recovery teams, users, vendors and VCCS personnel as required.
5. Review IT Environment.

Special Projects Team: (Attachment C 2.3)

- IT Staff
- Faculty Administrative Assistants (both campuses)
- Office Services Specialists, Procurement Staff (both campuses)
- Receptionists (both campuses)
- Fixed Asset Coordinator
- Buildings and Grounds Supervisors (both campuses)
- Any other personnel deemed necessary for this team

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

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Emergency Procedures

The Special Projects Team will have the following responsibilities:

1. Provide Transportation to and from backup facilities.
2. Make any Necessary telephone calls.
3. Order supplies, complete necessary paper work, and provide assistance as required to all support groups.

Customer Support Team: (Attachment C 2.3)

- IT Disaster Planning Coordinator
- Network Administrator
- Information Security Officer
- Installation and Repair Technicians
- Work Study students
- Any other personnel deemed necessary for this team

The Customer Support Team will have the following responsibilities:

1. Notify computer customers of the disaster and give them a timeframe for recovery.
2. Help customers develop or implement existing manual procedures for performing mission critical tasks.
3. Have customers prioritize normal tasks.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Priorities for reestablishment of services:

Based on the SVCC IT Contingency Planning and Business Recovery Program: *Business Impact Analysis* (Section B of the SVCC Security Plan), the priority for reestablishment of services is as follows:

1. Restore IT infrastructure
2. Academic
3. Admissions and Records
4. Payroll
5. Accounting
6. Accounts Payable
7. Financial Aid
8. Accounts Receivable
9. Learning Resource Center
10. Agency Management
11. Institutional Research and Planning
12. Budget and Planning
13. Administrative
14. Bookstore
15. Student Services
16. Auxiliary Operations
17. Buildings and Grounds
18. Purchasing
19. Fixed Assets
20. Grants and Development
21. Public Relations
22. Human Resources
23. Auditing
24. Food Service

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Maintaining the Plan

To be effective, the plan must be maintained in a prepared state that accurately reflects the current VCCS or individual college IT environment and current policies and procedures. It is essential that the plan be reviewed and updated regularly. The plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any part of the plan. Certain elements may require more frequent reviews (contact lists for example). SVCC will review its plan annually before June 15. The review will be conducted by the SVCC Security Committee.

The plan should be maintained at various locations and partial or complete copies provided to all appropriate team personnel. Because confidential and sensitive information may be contained in the plan, all team members should be instructed to house copies of the plan in a secure manner. The IT planning coordinator should maintain a list of all employees who have copies of the plan and where the partial or complete plan is housed. The SVCC list is as follows:

1. Mr. Will Hamilton, Planning Coordinator and ISO, will maintain copies of the plan in his office at the Daniel campus of SVCC; one hard copy and multiple electronic copies will be kept.
2. One hard copy and one electronic copy will be housed in the safe in the backup data storage facilities designated by SVCC. Each set of copies will be located in the Workforce Development Building for the respective campuses. The SVCC IT Network Services departments for the respective campuses will have the necessary information to open the safe and access the contents.

Formal Execution of the Disaster Recovery Plan

The President, DRP Coordinator, or designated successor as given in this document, may implement this disaster recovery plan. This plan is implemented based on known or anticipated threats and emergencies that may occur with or without warning. Southside

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Virginia Community College will use a time-phased approach for implementation whereby critical resources are deployed early and other resources will follow as needed.

- **Known threats and emergencies (with warning):** There are some threats to operations that may afford advance warning that will permit the orderly alert, notification, evacuation, and if necessary, the relocation of employees. Situations that might provide such warning include a thunderstorm, VCCS notification of a system outage, SVCC Planned outages, hurricane, and a transportation accident resulting in a threat of a release of hazardous material (HAZMAT) or a threat of a terrorist incident.

- **Unanticipated threats and emergencies (no warning) During Non-Duty Hours:** Incidents may not be preceded by warning, e.g., System failures, thunderstorms earthquakes, arson, HAZMAT, or terrorist incidents, and may occur while the majority of on-site staff is not at work. In these circumstances, while operations from the primary facilities may be impossible, the majority of our employees will still be able to respond to instructions, including the requirement to relocate following proper notification.

- **Unanticipated threats and emergencies (no warning) During Duty Hours:** Incidents may also occur with no warning during normal office hours. In these circumstances, execution of the Disaster Recovery Plan, if indicated by the circumstances of the event, would begin by execution of the Southside Virginia Community College's Crisis Management Plan (Attachment C 2.2) to support notification, evacuation, and situation assessment.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Essential Functions

Emergencies may occur both with and without warning which result in the:

- Loss of a facilities (Infrastructure)
- Loss of power
- Loss of telecommunications (Phones and Faxes)
- Loss of accessibility of information technology systems.
- Failure of server components such as a hard drive
- Failure of workstations
- Suddenly unavailable technical personnel

When confronting events which disrupt the normal operations of SVCC, the college is committed to provide essential functions which must be continued even under the most challenging emergency circumstances. SVCC has identified as essential functions only those most critical activities which ensure the safety and security of system users, employees, contractors, emergency responders and the general public; support the restoration of internal operations; and facilitate emergency response operations.

During activation of this Disaster Recovery Plan, all other activities will be suspended, to enable the agency to concentrate on providing the essential functions and building the internal capabilities necessary to increase and eventually restore operations. Appropriate communications with regular or expected users of services provided by those suspended services will be a priority.

SVCC has identified within the pages of the DRP, critical processes, services, systems, and equipment necessary to support each essential function, as well as key personnel required.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

The following types of scenarios have been identified by SVCC as the most likely to initiate the implementation of the Disaster Recovery Plan.

- **Planning Scenario 1: Loss of a facility.** Under this type of scenario, the Christanna campus is closed for normal business activities, but the cause of the disruption has not affected the Daniel Campus. The most likely causes of such disruption are: fire, system failure; hurricane, tornado, or explosion (regardless of cause) that produces no significant damage to the other facilities or systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities. Senior management, technical and supporting personnel working at the facility may be lost, injured, or not accounted for. From the technical perspective the infrastructure of this building will have to be rebuilt, new systems installed both for telecommunication and for the data network.

Procedures:

- *Loss of a facility procedures are contained in the College COOP plan. Relocating to an alternate facility would be SVCC's first option.*
- **Planning Scenario 2: Loss of Power.** Under this scenario, a campus loses power for a long period of time therefore cannot continue business as normal. The most likely causes of such disruption are: storms, fire, hurricane, tornado, or explosion (regardless of cause) that produces no significant damage to the other facilities or systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

In the event of a power failure Buildings and Grounds staff or Security would determine if this is a college problem. If not, VA Dominion

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- Power (888-667-3000) would be called to determine the details of the outage.
- Emergency lights for the hallways should activate during a power outage. An Emergency generator has been installed to provide limited A.C. power to critical college devices.
 - B&G will notify the appropriate SVCC senior management (depending on availability).
 - IT Network Service staff will take down all servers with a proper shutdown and notify VCCS of the outage.
 - If the outage is longer than 2 hours the appropriate SVCC senior management (depending on availability) will make the decision to allow student to leave and also make decisions regarding paid faculty and staff.
 - Buildings and grounds will continue to contact Va Power to acquire updates and let SVCC management know when the power is up.
 - IT Network Service Staff will bring back all systems and notify VCCS when the systems are up.
- **Planning Scenario 3: Loss of telecommunications (Phones).** Under this scenario, a campus loses all or a portion of phone and fax communications. The most likely causes of such disruption are: equipment malfunction, PSTN connection issues, storms, fire, hurricane, tornado, or human intervention (regardless of cause) that produces no significant damage to the other facilities or systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

- Two analog lines have been set up as backup communications for each campus in the event of power outages or a disaster that takes out our VoIP phone system. In the event that the analog line will not work, then cell

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

phones will be used in conjunction with B&G staff using hand radios.

Location of Analog lines:

Daniel Campus: Room 12a, (736- 2799) Room 71 (736-9650)
Christanna Campus: Room C 2 (949-7170) Room A 16 (949-7927)

- In some cases, the connection to the PSTN (local phone company) may still function, while native IP Telephony (calls routed as data) may not function. If this is the case, calls and faxes can still be made as toll calls until the problem is resolved.
- **Planning Scenario 4: Loss of accessibility of information technology systems. (server)** Under this scenario, a campus server that is critical to the business process of the college is unavailable. The most likely causes of such disruption are: hardware failure, fire, hurricane, tornado, or human intervention (regardless of cause) that produces no significant damage to the other facilities or systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

- Document the steps taken to troubleshoot and repair the system.
- Assuming the server is beyond repair; IT Network services would pull a spare server or call the appropriate vendor to do an emergency order. Using the documentation provided by SVCC IT Network staff; purchase a server with similar configurations as per purchasing procedures given later in this document.
- Bring up the replacement server and install the appropriate Server Operating System.
- Join the server to the appropriate domain.

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

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Emergency Procedures

- Pull the Hard Drive out of the Server that failed and try to get any data that may be on that hard drive or use that hard drive in the new cluster. If the hard drive is determined to be bad and once the server is in the domain, SVCC IT staff will perform the appropriate back up procedures for recovery of data.
 - All critical servers are set up using RAID arrays. Spare Drives are available.
 - If the hard drive failure is part of the mirrored set then a bad drive will be removed (HOT SWAPPED) and the server will be allowed to rebuild the mirrored set using a new drive.
 - If the hard drive is the data drive then all measures will be taken to try and salvage the data off this disk. If this is not possible then a backup restore will be applied for the last good backup. SVCC IT Network administrator's will initiate backup procedures.
-
- **Planning Scenario 5: Loss of accessibility of information technology systems. (router/switch)** Under this scenario, a campus edge device, core or other switch that is critical to the business process of the college is unavailable. The most likely causes of such disruption are: hardware failure, fire, hurricane, tornado, or human intervention (regardless of cause) that produces no significant damage to the other facilities or systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

- Document the steps taken to troubleshoot and repair the system.
- Assuming the device is beyond repair; IT Network services would configure a spare or call the appropriate vendor to do an emergency order. Using the documentation provided by SVCC IT Network staff, purchase a device with similar configurations as per purchasing procedures given later in this document.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- Bring up the replacement device and perform the appropriate configuration.
 - Install the new device on the network.
 - Test and verify the functionality of the new device.
- **Planning Scenario 6: Failure of workstations.** Under this scenario, an end users workstation is impacted and this end user is responsible for a critical business process of the college. The most likely causes of such disruptions include: system failure, hack attack, virus or other human intervention (regardless of cause) that produces no significant damage to the systems used by the agency. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

- Users are taught during Security Awareness training and new employee orientation to always store critical data on their Home drive, removable media, or the file server for the college. Consequently, no critical files should be lost if they are following proper procedures.
- In the event of a workstation failure and depending on the nature of the failure all measures will be taken to retrieve information stored locally on the end-users system (Parallel OS installs, Retrieval utilities and other system tools).
- In the event that data cannot be retrieved off the end-users system then the end users system will be replaced or re-imaged.
- If a system is replaced, the procedures given in the [SEC 514-03](#) will be followed for wiping the hard drive before surplus. If the hard drive cannot be accessed then the hard drive will be physically distressed ensuring total destruction of the hard drive.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- **Planning Scenario 7: Sudden unavailability of Technical Personnel.** Under this scenario, a disaster causing unavailability of key college technical staff has occurred. This type of event could significantly impact SVCC's communications, monitoring, and information technology capabilities.

Procedures:

- Emergency Delegation authority has been established in the event that certain IT personnel are not available and cannot be contacted. Succession of authority is given in the "When an IT disaster is recognized" section of this document.

Procedures for purchasing new hardware to support mission critical functions:

- Determine what hardware is needed. SVCC employees may use the IT Business Environment, and BIA documents to determine the type and specifications of hardware needed.
- Prioritize the equipment needed to support business functions by using the *priorities for reestablishment of services* guidelines given in this document.
- List and give specifications for all hardware needed.
- Obtain quotes from hardware vendors, as per vendor list (attachment C 2.3) or any other applicable documentation.
- Send quotes to the IT department purchasing agent.
- The IT department's purchasing agent will generate purchase orders for equipment.
- All documentation will be approved and signed by the Vice President of IT or VP of Finance.
- Order, receive, and document hardware as needed.
- Implementation of emergency procurement procedures must be consistent with the Department of General Services' Agency Procurement and Surplus Property Manual.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

Procedures for restoring critical software/applications:

- Determine what operating systems and applications are needed to support mission critical functions. SVCC employees may reference the IT Business environment, approved software lists, and BIA documents to determine the type and specifications of the software needed.
- Prioritize the software needed to support critical functions by using the *priorities for reestablishment of services* guidelines given in this document.
- Install operating systems using the proper media; all appropriate service packs and patches must be applied.
- Install applications from appropriate media. All software should be at the proper release level, and have the proper licensing documentation.
- Restore any necessary files from backup media.
- Test the operating systems and applications on the hardware before deploying to SVCC users.
- Upon completion of testing, approve the systems for use by end users.

Procedure for restoring non-critical software/applications:

- Determine what software/applications are needed to support non-mission critical functions. SVCC employees may reference the IT Business environment, approved software lists, and BIA documents to determine the type and specifications of the software needed.
- Prioritize the software needed to support non-critical functions by using the *priorities for reestablishment of services* guidelines given in this document.
- Install operating systems using the proper media; all appropriate service packs and patches must be applied.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- Install applications from appropriate media. All software should be at the proper release level, and have the proper licensing documentation.
- Restore any necessary files from backup media.
- Test the operating systems and applications on the hardware before deploying to SVCC users.
- Upon completion of testing, approve the systems for use by end users.

Procedure for restoring 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 the event of a hardware failure for the above mentioned equipment, the following procedure is initiated:

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 the Internet access is down.

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.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

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)**—Customer 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. The customer 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. The customer and Cisco are willing to commit resources during normal business hours to restore satisfactory service.
- **Priority 4 (P4)**—Customer requires 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.*

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- 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 to submit insurance claim. Ph (804) 786-3152 (select option 1).
- 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

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

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 equipment.
- The SVCC IT Network Administrators maintain a backup configuration of every Cisco device on the SVCC network.

System Servers:

Servers covered under the 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 affected servers will be replaced with a new server and a new four year maintenance service contract (as practicable and as budgeted for).

When an SVCC server fails due to a hardware problem, the SVCC IT network staff will call server support and provide the server's serial number to the technical support technician. The replacement part will be delivered the next business day. The 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 that are not covered by maintenance, damaged or destroyed by fire, flood, hurricane, earthquake, or due to theft:

The various server 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.
- 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 appropriate manufacturer to place an order to replace affected servers.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning: *IT Disaster Recovery Planning*

Emergency Procedures

- 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 stored in a fireproof safe on and off campus.

User Desktops:

SVCC main campus and off campus workstations covered under Maintenance Service Agreements:

Any Dell workstation computer that has a system hardware failure that is covered under the 4 year Dell Maintenance Service Agreement, will receive a replacement part by the next business day. When an SVCC desktop computer, covered under the 4 year Dell Maintenance Service Agreement fails due to a hardware problem, the SVCC IT Network staff desktop staff will call the Dell Desktop hotline at (800) 234-1490, provide the Dell desktop computer service tax number and express service code to the Dell Technical Support technician. The replacement part will be delivered the next business day. The Dell service technician will be onsite the next business day to install the replacement part.

SVCC main campus and off campus workstations not covered under Maintenance Service Agreements:

Any workstation computer that has a system hardware failure and is not covered under the 4 year Dell Maintenance Service Agreement will be analyzed by the SVCC IT Network staff to determine the extent of the computer problem. Once diagnosed, the hardware replacement part will be ordered through the Dell Corporation Parts website at www.dell.com. Replacement of the failed components can take up to one week. Typically, SVCC will replace desktop computers within three to four years in compliance with the useful life definitions of personal computer hardware and software recommended by the VCCS Technology Council and approved by the Advisory Council of Presidents.

Replacement of Dell (or other) workstations that are damaged or destroyed by fire, flood, hurricane, earthquake, or due to theft:

The Dell desktop maintenance service agreement does not cover equipment stolen or destroyed due to fire, flood, hurricane, earthquake, or by any other external force. In

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

**IT Contingency Planning: *IT Disaster Recovery
Planning***

Emergency Procedures

order to recover from such a catastrophic event, the SVCC IT Network Services Department 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 to submit insurance claim. Ph (804) 786-3152 (select option 1).
- Contact Dell Corporation and place an order to replace the workstations. Workstations will usually be delivered within one business week.
- The SVCC IT Network Services Department desktop staff will install the desktop computers and restore the desktop configuration, applications, and data files from the server backup tapes stored on and off campus.