

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

IT Contingency Planning includes developing plans to minimize the disruptions of critical functions and the capability to recover critical IT systems in accordance with [COV ITRM 501-01](#). The outcome may contribute to various plans that properly organize the response, recovery, and continuity activities for disruptions affecting the relationship between IT systems and business processes supported by the IT systems.

Once the Business Impact Analysis and Risk Assessment processes are complete, the business processes and supporting IT systems have been identified along with system vulnerabilities, threats, and current controls. The order of restoration has also been identified in these processes. This step involves using this information to ensure the contingency plan is able to address the risks completely and effectively.

### **Requirements:**

The following requirements must be addressed in the plan. The recommendations outlined at the end of this document define a minimum set of expectations. The VCCS and individual college may follow their own format as long as the requirements are met. The final plan must be approved by SVCC President's staff. Documentation of the IT Disaster Recovery Plan's approval will be included in the *IT Disaster Recovery Planning*, Disaster Recovery Plan Approval form. (Attachment C 2.3) Copies of the completed form will be maintained by the college ISO.

**Requirement:** Develop and maintain an IT Disaster Recovery Plan that supports restoration of essential business processes. The SVCC IT Disaster Recovery Plan is contained within Section C of the SVCC IT Security Plan, and all associated appurtenances thereto.

**Requirement:** Perform a periodic review, reassessment, testing and revision of the plan to reflect changes in business processes, services, IT systems, and personnel. "Periodic" must be defined in the System Office or College security plan but should be as a minimum on an annual basis. SVCC will do reassessment, testing and revision (as needed) of the Disaster Recovery Plan annually before June 15. Testing will be done by all appropriate team members or designees using the *DRP and COOP Plan Testing* document (Attachment C 2.1). The results will be reviewed and approved by the SVCC Security Committee using the *Recovery Plan Evaluation* form. (Attachment C 2.1) All copies of the documents will be maintained by the College ISO.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

**Requirement:** Provide training of all team members as part of the Security Awareness and Training Program. Each team member will be informed of his or her responsibilities via Managed Ongoing Awareness Training (M.O.A.T.) Security Awareness Training. M.O.A.T. will certify that these individuals have received, read and understood their responsibilities with respect to IT Security generally, and the Disaster Recovery Plan specifically.

**Requirement:** Establish alternate communication methods to support IT system user local and remote access to systems. In order to satisfy this requirement, this plan must work in conjunction with the SVCC COOP Plan. The COOP plan designates that the surviving main campus site will be used for both physical and logical alternative activities to support mission critical business processes. During outages that last for short periods of time, or for time periods not lengthy enough to invoke the COOP, manual procedures for mission critical business activities have been defined. These procedures, which were promulgated by the activity and system owners for each, are given in the *Manual Procedures for Mission Critical Business Functions* document. This document is located in Attachment C 2.1.

### **Recommended Processes**

#### **Definitions**

A disaster can be defined as a total or partial loss of any or all of the following: physical space, servers, workstations, network infrastructure equipment, personnel, software eradication, or hostile intrusion of the IT system resources resulting in an interruption of services.

A recovery plan is a manual with procedures, responsibilities, and critical information required to execute a recovery of IT systems that support critical and essential business functions. The SVCC DRP was developed in conjunction with the College's *Crisis Management Plan* (Attachment C 2.2) to allow a rapid and organized response to the full or partial destruction of the College's IT capabilities.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

### **Assumptions**

The SVCC Disaster recovery Plan was developed based on the following assumptions:

- One of the College sites will survive the disaster.
- All resources and staff can be made available as soon as possible.
- All members of the disaster recovery teams have access to the most current copies of the disaster recovery plan.
- Users will continue to operate via a manual mode until IT services can be restored.
- Backup media and documentation will have also survived and will be made available as soon as possible.
- Service agreements with outside entities have been maintained.
- In the event of total or partial loss of the College's IT Staff, assistance will be available from VCCS personnel to implement the Disaster Recovery Plan.

### **Information Technology Environment**

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location of all campuses, building plans indicating general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures (reference [IT System and Data Backup and Restoration](#), Section C 3 of the SVCC IT Security Plan). Provide a diagram of the architecture, including security controls and telecommunications connections. This information and all associated diagrams are developed, maintained, and documented by the SVCC IT Network Administrators and staff.

### **When an IT Disaster is Recognized**

State the course of actions that should occur when a disaster is recognized. The following is an example of the initial flow once a disaster has been 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. Peter Hunt, Mr. Bob Upson, Mr. John Turner. The IT

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

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.

### **IT Disaster Recovery Teams**

Disaster recovery teams will be utilized to restore automated IT system services. The recovery teams will be lead by the IT disaster planning coordinator and will participate in recovery activities based on the level of severity of the loss, recovery deemed necessary, and restoration order as deemed in the Business Impact Analysis and Risk Assessment processes. Depending on the size of the agency, employees may be assigned to various teams and assigned multiple roles and responsibilities. The teams and members are listed in the IT Contingency Planning: *IT Disaster Recovery Planning*, Disaster Recovery Teams documents. (Attachment C 2.3)

### ***IT Disaster Planning Coordinator***

Determine the IT disaster planning coordinator and the backup coordinators in order of succession. List the name, position, and contact information of each coordinator. List the responsibilities of the coordinator. The Planning coordinator is Mr. Will Hamilton Phone: 434-736-2028 email: will.hamilton@southside.edu. The backup coordinator is Dr. Linda Sheffield. Phone: 434-736-2000, email: linda.sheffield@southside.edu.

Coordinator responsibilities include:

- Manage and coordinate all IT disaster plan activities.
- Contact all IT disaster recovery team members involved in the recovery effort.
- Ensure all IT disaster recovery team members have a copy of the plan.
- Appoint replacement staff if necessary.
- Initiate tasks as delegated by IT disaster recovery team responsibilities.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

- Provide IT disaster recovery status via communication with College President, Provosts, and/or VCCS administrators and other disaster recovery teams.
- If necessary, assist planning for returning to normal conditions (renovations, new construction, etc.).

### ***IT Emergency Management Team***

Determine the members of the IT Emergency Management Team and list the appropriate responsibilities. IT Contingency Planning: *IT Disaster Recovery Planning*, Emergency Management Team document. (Attachment C 2.3)

The SVCC team consists of the following personnel:

- IT Disaster Planning Coordinator
- Network Administrator
- Information Security Officer
- College President
- College Provost
- Buildings and Grounds Supervisor
- Administrative, Financial, and Facilities Management Department Head
- Any other personnel deemed necessary for this team

Responsibilities of the IT Emergency Management Team include:

- Assessment of the damage.
- Provide a detail status of the disaster to the disaster planning coordinator as soon as possible.
- Contact all vendors, contractors or external resources necessary to restore services to the damaged areas.
- Provide a general status of the disaster to college personnel.
- Determine the priorities. There should be a minimal accepted time frame the college will function with degraded operations before the backup plan is implemented.
- Ensure all needed support staff is contacted to provide assistance.
- Determine a general time frame for when all services will be restored.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

### ***IT Technical Support Team***

Determine the members of the IT Technical Support Team and list the appropriate responsibilities. IT Contingency Planning: *IT Disaster Recovery Planning*, IT Technical Support Team document. (Attachment C 2.3)

The SVCC team consists of the following personnel:

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

Responsibilities of the IT Technical Support Team include:

- Working with the IT Emergency Management Team to conduct an on-site assessment of the damaged area to determine the condition of IT resources.
- Determine what computer hardware/software has been damaged.
- Review the risk assessment analysis and business impact analysis and determine what the critical/non-critical applications are and to determine whom is responsible for each application.
- List procedures to create a new environment for the hardware or for the purchase of new hardware (Procedures given in the IT Contingency Planning: *IT Disaster Recovery Planning*, Emergency Procedures document, Section C 2).
- List procedures to restore critical software/applications. (Procedures given in the IT Contingency Planning: *IT Disaster Recovery Planning*, Emergency Procedures document, Section C 2).
- List procedures to restore non-critical software/applications. (Procedures given in the IT Contingency Planning: *IT Disaster Recovery Planning*, Emergency Procedures document, Section C 2).
- Contact application owners to determine their role in the recovery process.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

### ***Special Projects Team***

Determine the members of the Special Projects Team and list the appropriate responsibilities. IT Contingency Planning: *IT Disaster Recovery Planning*, Special Projects Team document. (Attachment C 2.3)

The SVCC team consists of the following personnel:

- 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

Responsibilities of the Special Projects Team include:

- Providing transportation to and from backup facilities, external vendors or other off-site locations.
- Assisting in making telephone calls as needed.
- Coordinating packing and moving supplies as needed.
- Acquiring emergency purchasing means (i.e. assigning purchasing charge card or delegated purchasing authority) or being available to purchase goods or services as needed.
- Providing clerical support as needed.

### ***Customer Support Team***

Determine the members of the Customer Support Team and list the appropriate responsibilities. . IT Contingency Planning: *IT Disaster Recovery Planning*, Customer Support Team document. (Attachment C 2.3)

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

The SVCC team consists of the following personnel:

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

Responsibilities of the Customer Support Team include:

- Notifying IT customers of the disaster and giving them a time frame for recovery.
- Assisting customers in developing manual procedures to accomplish work if resources are unavailable for a long period of time.
- Assisting users with hardware and software restoration or relocation to an alternate office site.
- Have IT customers list the priority of their day to day tasks.

### **Emergency Response Procedures**

List the emergency response procedures appropriate to any incident or activity, which may endanger lives, property or the capability to perform essential functions. This may include the bulleted items below:

- SVCC Crisis Management Plan (Attachment C 2.2)
- The detailed technical procedures for installing and configuring systems at an alternate site. These procedures are outlined in the IT Contingency Planning: *IT Disaster Recovery Planning, Emergency Procedures* document.
- The detailed technical procedures for restoring systems from backup media. The procedures written by SVCC IT Network Administrators are located in Attachment C 3.1.
- The procedures for returning to normal operations once on-site facilities are under normal operations. These procedures are outlined in the IT Contingency Planning: *IT Disaster Recovery Planning, Emergency Procedures* document, *Priorities for Reestablishment of Services* section.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

- Documented procedures for emergency access authorization to VCCS or individual college facilities in the event of an emergency of disaster. The SVCC Disaster Planning Coordinator or designee will reference the Authorized Access Personnel list as referenced in Facilities Security: *Physical Security* (Attachment G 1.1) and the IT Vendor list as per IT Contingency Planning: *IT Disaster Recovery Planning, Vendor List* document, (Attachment C 2.3). If access needs to be granted to personnel not included on these lists, emergency access will be granted to the requesting party by the Planning Coordinator or designee via the use of the Emergency Access Authorization form located in Facilities Security: *Physical Security* (Attachment G 1.1) The Planning Coordinator will maintain copies of the completed form.

**Emergency Telephone List:** Maintain a list of all emergency service telephone numbers in your area. This may include fire, police, rescue squad, and applicable State and Local Government entities. The list as designated by SVCC is located in the IT Contingency Planning: *IT Disaster Recovery Planning, Emergency Telephone List* document. (Attachment C 2.3)

Maintain a list of all IT disaster recovery teams. The list should contain all work location numbers, cellular or pager numbers, email addresses, home numbers, etc. Update the list as employees enter or depart the VCCS or college. The list is located in the IT Contingency Planning: *IT Disaster Recovery Planning, DRP Team* documents. (Attachment C 2.3)

Maintain a list of all IT related vendors (hardware and software vendors, various IT state contract vendors, telecommunications vendors, other state agencies, etc.) The list is located in the IT Contingency Planning: *IT Disaster Recovery Planning, IT Vendor List* document. (Attachment C 2.3)

### **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 using the

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

Recovery Plan Review Form (Attachment C 2.3). Copies of the review form will be maintained by the college ISO.

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 the plan in a secure manner. The IT planning coordinator will maintain a list of all employees who have copies of the plan and where the partial or complete plan is housed. The list of employees who have copies of the plan, and the location of the plan copies are given in the *SVCC Disaster Recovery Plan Maintenance* document. (Attachment C 2.3)

The plan should reference specialized training for all disaster recovery team members. Training may include the purpose of the plan, cross team coordination and communication procedures, reporting procedures, security requirements, and team specific and individual processes during each phase of the disaster. SVCC will require that the Disaster Recovery Plan be tested annually, and that all team members be reminded of their responsibilities during the testing and evaluation of the plan. These employees will also be reminded of their individual and collective duties and responsibilities with respect to security generally and the Disaster Recovery Plan specifically as a part of the SVCC Security Awareness Training program. The information contained in these reminders is given in the *IT Contingency Planning: IT Disaster Recovery Planning, Emergency Procedures* document, team responsibilities items.

The plan should reference annual training for general staff members when responding to an emergency situation such as fire, inclement weather, and other incidents requiring a shut down of IT operations and relocation to an alternate site. The SVCC Faculty and Staff Handbook (Sections 2.9 and 2.11) gives the policies and procedures to be followed with respect to the issues mentioned above. These situations are also mentioned in the SVCC Crisis Management and COOP plans and will be referenced in the SVCC annual Security Awareness Training program.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

### **Plan Testing**

Plan testing is a critical element of the IT disaster recovery plan. Testing should be done at least once a year and more often as necessary. SVCC will test the plan annually before June 15 using the *DRP and COOP Plan testing* document (Attachment C 2.1). The various Disaster Recovery Teams will perform the testing and the results will be reviewed by the SVCC Security Committee. Testing assists in identifying and addressing deficiencies. Testing also helps evaluate the ability of recovery teams to implement the plan quickly and efficiently. The following components will be addressed during the SVCC IT Disaster Recovery Plan test:

- Testing coordination among recovery teams
- Testing notification procedures

The purpose of testing is to demonstrate to both management and recovery teams the ability of one or more vital business processes to continue functioning inside the identified timeframe post a business interruption event. An exercise is not a pass/fail work effort but an opportunity to identify vulnerabilities and gaps in your recovery plan.

Testing may be in performed in various formats.

### **Tabletop Exercises**

A tabletop exercise simulates an emergency situation in an informal, stress-free environment. The participants gather around a table to discuss general problems and procedures in the context of an emergency scenario. The focus is on training and familiarization with roles, procedures, or responsibilities.

### **Functional Exercise**

The functional exercise simulates an emergency in the most realistic manner possible, short of moving real people and equipment to an actual site. As the name suggests, its goal is to test or evaluate the capability of one or more functions in the context of an actual disaster.

---

# SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

---

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

### **Full Scale Exercise**

A full-scale exercise is as close to the real thing as possible. It is a lengthy exercise which involves numerous groups participating and using the equipment and personnel that would be called upon in a real event. The full-scale exercise may be held at several locations. A full scale exercise may not be feasible since the risk of bringing down current systems exists.

All testing formats should involve a question and answer session and a review session. Information collected during an exercise, and discussed during a review of the exercise, that improves plan effectiveness should be incorporated into a revised version of the IT disaster plan.

SVCC will perform Tabletop Exercises as its testing mechanism for the Disaster Recovery Plan. The recovery strategy for a business activity will be tested using the *DRP and COOP Plan Testing* document and evaluated using the *Recovery Strategy Evaluation* form. (Attachments C 2.1 and C 1.1 respectively)

The strategy will be implemented by the various recovery teams, reviewed by the SVCC Disaster Recovery Planning Coordinator and the SVCC Security Committee. Upon completion of the exercise, the Disaster Recovery Plan will be evaluated using the *Recovery Plan Evaluation* form. (Attachment C 2.1) The plan will be reviewed and evaluated by the Disaster Recovery Teams, the Disaster Planning Coordinator, and the SVCC Security Committee. All testing, reviews, and evaluations will be completed annually prior to June 15. The College ISO will maintain records of all evaluation results.