
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning *IT System and Data Backup and Restoration*

In accordance with the [COV ITRM 501-01](#), an IT System and Data Backup Restoration Plan must be implemented to create a comprehensive backup plan including standards and operational procedures executed during a system backup. This plan shall also include standards and operational procedures executed during system restoration.

An IT System and Data Backup and Restoration plan is mandatory for ensuring the availability and reliability of VCCS and individual college data. The implementation and documentation of this plan is the responsibility of the SVCC IT Network Administrators. Various backup systems, media, and methods may be used to create a comprehensive backup plan. Impacts from the Business Impact Analysis and Risk Assessment processes should be reviewed to assist in determining backup priorities.

Requirement

Store all media backups off site in a secure, environmentally controlled facility. The alternate site should be located far enough away from the primary site to reduce the likelihood of one disaster affecting all sites. All backup media should be uniquely labeled so that media can be quickly obtained in the event of an emergency. Provide the address and emergency contact information for the alternate facility. SVCC maintains copies of backup media in fireproof safes located in the Workforce Development Buildings at each campus. The media is labeled as per the SVCC IT Network Administrators' instructions. The physical locations and contact information regarding the backup media are as follows:

Christanna Campus: 109 Campus Drive,
WFD building,
Alberta, VA 23821
IT Network Administrator: Mr. John Turner
IT Network Administrator Phone: 434-949-1033

Daniel Campus: 200 Daniel Road
WFD Building
Keysville, VA 23947
IT Network Administrator: Mr. Bob Upson
IT Network Administrator Phone: 434-736-2009

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Contingency Planning *IT System and Data Backup and Restoration*

Requirement

Only authorized personnel should perform backups and restoration. Authorized personnel must review backup logs after the completion of each backup to verify that the backup was successful. This person should be different from the person who performed the backup to verify that the backup was completed properly. The System Owner must designate all personnel who are authorized to perform backups and reviews. The System Owners for the SVCC IT Networks and all associated functions are the IT Network Administrators, and as such, will designate and document the personnel who are authorized to do backups and reviews of the same. A list of all authorized IT personnel is located in Section H, Attachment H 1.1, of the SVCC IT Security Plan.

Requirement:

Backup schedules must be documented and approved by the System Owner. The System Owners for all SVCC IT Systems are the IT Network Administrators. As the System Owner they will perform the following operations: For each system and data type, identify and document the backup schedule and type of backup used. Type of backup information in the schedule may include:

- Frequency (hourly, daily, weekly, monthly).
- Full, incremental, or differential backup.
- Type of backup media. This is dependent on what is being backed up. A backup of PC data most likely requires different media and methods than a backup of servers.
 - PC backup media and methods may include floppy disks, tape drives, removable cartridges, compact disks, replication, and imaging.
 - Server backup media and methods may include RAID (mirroring, parity, striping), electronic vaulting, server load balancing, disk replication (synchronous or mirroring, asynchronous or shadowing), and storage virtualization.

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

IT Contingency Planning
IT System and Data Backup and Restoration

Requirement

The System Owners for all SVCC IT Systems are the IT Network Administrators. Network Emergency backup and restoration operation procedures must be documented, reviewed, and approved by the System Owner. The System Owner should be identified and included in all contingency planning processes for emergency backup and restoration.

Requirement

Proper electronic (encryption measures for example) or physical security measures (additional insurance or locked transport case for example) must be taken for all backup media that is sent electronically, mailed, or physically transported off site. SVCC will use proper encryption and physical security measures as indicated in the Data Protection standard. (Section F of the SVCC IT Security Plan)