
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Data Storage Media Protection*

In accordance with the [COV ITRM 501-01](#), Data Storage Media Protection identifies the steps required for the appropriate handling of stored data to protect the System Office and College data from compromise.

SVCC IT Staff must document Data Storage Media protection best practices to include the requirements listed below.

Requirement:

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. All SVCC employees will be the Data Custodians responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

Requirement:

Sensitive data should not be stored on mobile storage media, [any non-network storage device or media](#), including laptops as well as any non-network drive, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head , [accepting all unmitigated risks](#) that includes the following elements: **(Jan 2010 Revision)**

- a. The business or technical justification;
- b. The scope, including quantification and duration (not to exceed one year)
- c. A description of all associated risks;
- d. Identification of controls to mitigate the risks, one of which must be encryption; and
- e. Identification of any unmitigated risks.

Note: *Agencies must apply these practices to sensitive data stored on all mobile data storage media, desktops and mobile workstations, CD's and USB Drives, except for backup media, including removable data storage media and the fixed disk drives of all mobile workstations, such as laptop and tablet computers. (Jan 2009 Revision)*

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Data Storage Media Protection*

This issue is addressed in the Data Protection: *Data Storage Media Protection* standard, *Mobile Device Protection Procedure* document. (Attachment F 1.1) Data storage media containing sensitive data must be physically and logically secured. Security awareness and training will be provided via M.O.A.T. to those employees who have approval to store such information on mobile devices at SVCC. Designation of these employees will be determined by SVCC President's staff and documented on the Mobile Device Security form (Attachment F1.1) in conformance with the Mobile Device Protection procedure.

SVCC must prohibit the connection of any mobile data storage media not owned by COV to any COV IT system, [unless the connection is to a segmented guest network. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract. \(Jan 2010 Revision\)](#)

SVCC must prohibit the storage of COV data on any mobile data storage media not owned by COV.

Storing of any Commonwealth data on non-COV owned or leased computing devices is prohibited due to records retention and Freedom of Information Act (FOIA) complexities, as well as the associated information security risks. [\(Jan 2010 Revision\)](#)

Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, and digital music players owned by employees, contractors, and students.

VCCS allows flexibility in meeting this requirement based on approval from Tech Council. Colleges who have a legitimate need for flexibility in complying with this requirement must complete form VCCSITSEC001 providing the justification.

Requirement:

SVCC restricts the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel only. [SVCC will Store off-site backup media in an off-site location that is geographically/separately distinct from primary location. \(Jan 2009 Revision\)](#)

Procedures must be implemented and documented to safeguard handling of all backup media containing **sensitive data**. Encryption of backup media shall be considered where the data is Personal Health Information (PHI) or Personally Identifiable Information (PII). Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented. [\(Jan 2009 Revision\)](#)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Data Storage Media Protection*

Sensitive data: [Personal Information](#) which means [a combination of a first name, or first initial, last name](#), and any of the following: Financial account number, credit or debit card number [and/or the corresponding password, security, or access codes](#).

Authorized Personnel are defined in the Personnel Security: *Access Determination and Control* and the Facilities Security: *Physical Security* standards, Authorized Access Personnel List (Attachments G 1.1 and H 1.1 respectively) SVCC shall require that all deposits and withdrawals of storage media located off-site be authorized by the SVCC IT Network Administrator(s) and logged using the Data Protection: *Data Storage Media Protection* Storage Media Log sheet (Attachment F 1.1) by personnel as defined above. SVCC IT staff will maintain documentation of all log sheets.

Requirement:

[Data storage media containing sensitive data must have logical and physical protection that is commensurate with sensitivity and risk. \(Jan 2009 Revision 4\)](#)

Authorized Personnel are defined in the Personnel Security: *Access Determination and Control* and the Facilities Security: *Physical Security* standards, Authorized Access Personnel List (Attachments G 1.1 and H 1.1 respectively) SVCC shall require that all deposits and withdrawals of storage media located off-site be authorized by the SVCC IT Network Administrator(s) and logged using the Data Protection: *Data Storage Media Protection* Storage Media Log sheet (Attachment F 1.1) by personnel as defined above. SVCC IT staff will maintain documentation of all log sheets.

Requirement:

[Document and exercise a strategy for testing disaster recovery procedures and that IT system and data backups are functioning as expected and the data is present in a usable form. \(Jan 2010 Revision\)](#)

The SVCC IT Network administrator will be responsible for satisfying this requirement and providing auditable documentation of the same.

Requirement:

SVCC shall adhere to the procedures in place to address the purging of all data, using software utilities or electromagnetic means, from magnetic storage media such as hard drives, removable disk drives, diskettes, CD-ROMs, zip drives, jump drives, personal

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

Data Protection – *Data Storage Media Protection*

digital assistances, and other storage media before they are discarded, in accordance with the [ITRM Standard SEC514-03](#) as given in the IT Asset Management: *IT Asset Control* standard, *procedure for removing data from surplus computer hard drives and electronic media*, document. (Section J 1, Attachment J 1.1)