
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Data Storage Media Protection*

Mobile Device 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.

Requirement:

Sensitive data should not be stored on mobile devices unless there is a documented business need. *Note: This does not apply to backup media transport.* This issue is addressed in the Data Protection: *Data Storage Media Protection* standard, Mobile Device Protection 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. The procedure to request transport of sensitive data via mobile device is as follows:

1. The employee must have the proper account access documentation as per the Logical Access Control: *Account Management* standard, procedure, and all associated forms. (Section E 1 and Attachment E 1.1)
2. The employees supervisor must generate a request via the Mobile Device Security Form (Attachment F 1.1) stating the nature and necessity of the function.
3. The form must be filled out and signed by the employee, the requesting supervisor, the IT Network Administrator, College President, and the College ISO.
4. Copies of completed form will be kept by the requesting supervisor and the SVCC IT Staff for audit purposes.
5. The device must be signed out and returned according to the IT Asset Management: *IT Asset Control* procedure and all associated forms. (Section J and Attachment J 1.1)