
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Encryption*

In accordance with the [COV ITRM 501-01](#), Encryption document the security related activities that must be adhered to in each phase of the development life cycle for System Office and College IT systems.

Encryption is an effective way to achieve data security. The System Office and Colleges should utilize encryption controls that commensurate with the sensitivity and risk of the data.

Requirement:

The System Office and Colleges should define and document practices for selecting and deploying encryption technologies. This may be as simple as researching the most recent software available in the current market. Deployment is dependent on the type of software selected, the system affected, and the appropriate time frame available to provide the least interruption to System Office or College personnel.

Where possible, individuals shall use only encrypted means of access for data [that is sensitive relative to confidentiality and integrity](#) via a public WAN such as the Internet. Where this is not possible, individuals shall not pass sensitive college information.

Encryption methods shall use at least 128 bit encryption keys, with large encryption keys preferred. (Jan 2009 revision)

Requirement:

Commensurate with sensitivity and risk, the SVCC IT Network Administrator [or the SVCC service provider](#) shall:

[Require encryption during transmission of sensitive data over non-Commonwealth networks or any public accessible networks.](#) (Jan 2010 Revision)

[Transmission of sensitive data \(such as credit card numbers, social security numbers, passwords, PII\) is required to be encrypted to a level that is commensurate with its sensitivity and risk.](#) (Jan 2009 Revision)

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.](#) (Jan 2009 Revision)

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Data Protection – *Encryption*

Requirement:

The System Office and College should provide technical training required to users on the proper use of encryption products. SVCC IT staff will be trained in the use of products used for encryption. The IT Network Administrator will be responsible for selection of and training for the encryption product.

Requirement:

SVCC IT Network administrators shall use appropriate processes and these processes should be documented prior to implementing encryption:

- The SVCC Incident Response Plan (Section I 2, Attachment I 2.1) includes actions to be taken when keys are compromised.
- SVCC IT Network Administrators will be responsible for administration and distribution of encryption keys via a secure key management system.
- Encryption keys should only be generated through an approved encryption package as defined in requirement two above.
- SVCC IT staff shall make sure that encryption keys are securely stored.