SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN

Logical Access Control
Mobile Computing Policy

In accordance with VCCS Security Standard 11.7, *Mobile Computing*, VCCS should ensure that the protection required is commensurate with the risks that mobile computing and teleworking causes. When using mobile computing, the risks of working in an unprotected environment will be considered and appropriate protection applied. In the case of teleworking VCCS will apply protection to the teleworking site (location) and ensure that suitable arrangements are in place for this way of working.

A formal policy should be in place, and appropriate security measures should be adopted to protect against the risk of using mobile computing and communication facilities. Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home-working/teleworking or being transported away from the normal work location.

In meeting these requirements SVCC has adopted the following controls:

1. The custodian of the device will be responsible for assuring the physical protection, access controls, cryptographic techniques, back-ups, and virus protection for the device.

2. Physical protection: Equipment carrying important, sensitive, and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

3. Access controls: Local device authentication will consist of username, password, and /or PIN number depending on the device.

4. Cryptographic techniques: Remote access to SVCC production networks will be done using a VPN with appropriate authentication and encryption techniques. Mission critical or sensitive data will be stored on encrypted drives. Encryption methods will be determined and implemented using industry best practices by the SVCC IT Network Administrator.

5. Backups: All data will be backed up at regular intervals, with mission critical or sensitive data being backed up at least weekly.

Logical Access Control

Mobile Computing Policy

6. Virus and malware protection: All mobile devices will have *at least* anti-virus software installed and updated regularly. Additionally, anti-spyware and personal firewall software should be considered for all devices.

Note: In addition, all IT security policies, procedures, and controls as set forth in the SVCC Security Plan will be enforced pertaining to mobile devices and teleworking.