Data Protection – *Data Storage Media Protection*

**PURPOSE**

In accordance with the VCCS Security Standards 10.7, *Media Handling*, and 10.8, *Exchange of Information*, 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. VCCS should consider the security implications associated with controlling and protecting sensitive, confidential, and proprietary information on electronic and non-electronic media by establishing effective operating procedures to protect and dispose of removable media (tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media etc.), input and output data, and system documentation from unauthorized disclosure, modification, removal, and destruction. 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.

**Requirement: Management of Removable Media §10.7.1**

VCCS and Colleges will protect information by implementing effective procedures to manage electronic and non-electronic removable media including the handling of assets.

In meeting this requirement, SVCC has adopted the following controls:

Data Owners are responsible for the protection of stored sensitive data. Data Owners are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage.

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.

- See [SVCC Security Policies](#), Policy 6.1, *Data Protection*
- Also see *Data Storage Media Protection* document, Section F 1, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management
Data Protection – *Data Storage Media Protection*

- See SVCC Standard 11.3, *User Responsibilities*. Location: Security\SVCC ISO 27002 2011\Phase II documentation\SVCC Phase II 11 Access Control

**Requirement: Information Handling Procedures §10.7.3**

The VCCS System Office and Colleges will protect information by implementing procedures for the handling and storage of information to prevent unauthorized or inadvertent disclosure or misuse. These procedures will include operating procedures and will apply to information in paper form, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services and facilities, use of fax machines, other devices or formats, and will include the handling, processing, storing, and communicating of information consistent the criticality and sensitivity of the information.

In meeting this requirement, SVCC has adopted the following controls:

All sensitive information shall be labeled either [confidential] or [internal use only] in the document containing the sensitive information; confidential and internal use only documents are not accessible to the general public. 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. Access restrictions in place to prevent access by unauthorized personnel based on least privilege as defined in the BIA process. Review of employee IT roles and responsibilities at regular intervals and as part of the SVCC BIA process.

- See [SVCC Security Policies](#), Policy 6.1, *Data Protection*
- Also see *Data Storage Media Protection* document, Section F 1, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management.
Data Protection – *Data Storage Media Protection*

**Requirement: Security of System Documentation §10.7.4**

The System Office and Colleges will protect all system documentation against unauthorized access. System documentation may contain a range of sensitive information, e.g. descriptions of applications, processes, procedures, data structures, authorization processes.

In meeting this requirement, SVCC has adopted the following controls:

- System documentation should be stored securely in locked containers; password protected, or encrypted media. System Owners or designees are responsible for system documentation.
- The access personnel for system documentation should be kept to a minimum and authorized by the System, Data, or Application Owner.
- System documentation held on a public network, or supplied via a public network, will be appropriately protected.

- See SVCC Security Policies, Policy 6.1, *Data Protection*
- Also see *Data Storage Media Protection* document, Section F 1, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management.

**Requirement: Physical Media in Transit §10.8.3**

The VCCS System Office and Colleges will protect media containing sensitive or confidential information against unauthorized access, misuse, or corruption during transportation beyond the System Office or College physical boundaries. Information can be vulnerable to unauthorized access, misuse, or corruption during physical transport, for instance when sending media via the postal service or via courier.

In meeting this requirement, SVCC has adopted the following controls:

The following items will be considered to protect information and media being transported between sites:

- Reliable transport or couriers will be used, for example US Postal Service or UPS.
Data Protection – *Data Storage Media Protection*

- Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers’ specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media’s restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;
- Where necessary, controls and procedures will be adopted to protect sensitive information from unauthorized disclosure or modification; examples include:
  - Use of locked containers;
  - Delivery by hand by authorized individuals;
  - Tamper-evident packaging (which reveals any attempt to gain access);
  - In exceptional cases, splitting of the consignment into more than one delivery and dispatching by different routes.

- Also see *Data Storage Media Protection* document, Section F 1, SVCC Security Plan. Location: Security\SVCC ISO 27002 2011\Phase III documentation\SVCC Phase III\10 Communications and Operations Management.