
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *IT Systems Interoperability*

In accordance with the [COV ITRM 501-01](#), IT systems interoperability security requirements identify the steps necessary for protecting data shared with external IT systems.

A system interconnection may be defined as the **direct connection of IT systems** for the purpose of sharing data. This does not include instances where data is shared via tape or file exchanges. Interconnecting IT systems can have security consequences and may expose the VCCS to potential risks. The following recommendations are provided as minimum guidelines. Colleges are encouraged to apply additional safeguards that commensurate with the risks identified for the applicable IT system and associated data.

Note: SVCC only connects to enterprise systems and applications owned by the VCCS; no other system interoperability is required.

Requirement:

The System Owner and Data Owner must document the following information for interconnected systems: SVCC uses the IT Systems Security: *IT Systems Interoperability*, System Logging Form (Attachment D 2.1) to satisfy this requirement.

- Name of interconnected systems.
- The types of shared data.
- The direction in which data flows (one-way or both ways).
- The System Owner, Information Security Officer, and System Administrator name and contact information of the entity that owns the IT system which shares the data.

Note; titles of these personnel may vary depending on the entity that owns the interconnected IT system.

It is critical that the System Office and Colleges document as much information as possible about the interconnection.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *IT Systems Interoperability*

Requirement:

The System Office and Colleges must develop a written agreement that includes the following requirements: Reciprocal interoperability agreements should be promulgated by VCCS Enterprise Services and disseminated to all VCCS entities.

- Security controls that must be implemented to protect the confidentiality, integrity, and availability of data passed between interconnected systems.
- The Data Owners of each system must inform each other regarding *other* IT systems with which their IT systems interconnect or share data, and inform each other prior to establishing additional interconnections.
- Specify how the shared data will be stored on each IT system.
- Specify that System Owners of the IT systems acknowledge and agree to abide by any legal requirements for the handling, protection, and disclosure of the shared data.
- Provide authority for each Data Owner to approve access to the shared data.

Each System Owners must approve and enforce the written agreement.