
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT System and Data Sensitivity Classification*

The IT System and Data Sensitivity Classification is performed in conjunction with the Business Impact Analysis to determine the adverse impact of a security occurrence in terms of loss or degradation of integrity, availability, and confidentiality. This process will must also identify if the types of data are subject to other regulatory requirements. [The Data Owner for each type of IT system is required to provide this information to the Contingency Planning Coordinator using the various worksheets associated with BIA Template. Section B, SVCC Security Plan. \(July 2008 Revision\)](#)

The following requirements and recommendations are provided to assist with compliance of the Commonwealth of Virginia (COV) Information Technology Resource Management Standard, [COV ITRM 501-01](#) standards for IT system and Data Sensitivity Classification. Worksheet two of the Business Impact Analysis Template may be used to assist in this process. (Attachment B 2.1b SVCC IT Security Plan)

Requirement:

Worksheet one of the [Business Impact Analysis Template](#) identified the activities and core functions of each business unit. Worksheet two must determine the potential damages to the VCCS or college of a compromise using the sensitivity criteria in the table below. [The Data Owner for each type of IT system is required to complete worksheet two. \(July 2008 Revision\)](#) The completed Business Impact Analysis Template is located in Attachments B 2.1a, B 2.1b, and B 2.1c of the SVCC IT Security Plan.

Loss of: **May result in:**

Confidentiality System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT System and Data Sensitivity Classification*

Integrity System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

Availability If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Apply each criterion above to all systems and data and measure the impact using the magnitude of impact table below. This analysis will assist in prioritizing risks and identifying areas for immediate improvement in addressing the vulnerabilities.

Magnitude of Impact

Low - May result in the loss of some tangible assets or resources or may affect mission, reputation, or interest.

Medium - May result in costly loss of tangible assets or resources, may violate, harm or impede mission, reputation, or interest, or may result in human injury.

High - may result in costly loss of major tangible assets or resources, may significantly violate, harm or impede a mission, reputation or interest, or may result in human death or serious injury.

Note: A system/data should be considered sensitive if any of the three criteria contain a moderate or high rating.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Contingency Planning and Business Recovery Program *IT System and Data Sensitivity Classification*

Requirement:

- Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications. (July 2007 Revision) This requirement is met during the BIA process and is validated by the BIA and RA Executive Summary located in Attachment B 2.1.
- Verify and validate that all agency IT systems and data have been classified for Sensitivity This requirement is met during the BIA process and is validated by the BIA and RA Executive Summary located in Attachment B 2.1.
- Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users. (July 2007 Revision) This requirement is addressed in the SVCC It Security Roles and Responsibilities document, section B 1.
- Require that the agency prohibit posting any data classified as sensitive based on confidentiality (Jan 2009 Revision) on a public web site unless a written exception is approved by the Agency Head identifying the business case, risk risks, mitigating logical and physical controls, and any residual risk.
SVCC Policy as per Faculty / Staff Handbook, section 5.2.3.

Requirement:

(Jan 1, 2009 Revisions)

- Identify or require that the Data Owner identify the type(s) of data handled by the IT system, whether the data is subject to other regulatory requirements, and determine or require the Data Owner determine the potential damages to the agency in the event of a compromise of confidentiality, integrity, or availability of each type of data handled by the IT system. (BIA process, Section B2)
- System Office and colleges shall review IT system and data classifications with the College President, Chancellor, or designee, and obtain approval of these classifications. Verify and validate that all agency IT systems and data have been classified for sensitivity. (BIA process, Section B2)
- Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users. (BIA process, Section B2)
- The System Office and colleges shall prohibit posting any data classified as sensitive on a public web site. (Section 6.1, Data Protection SVCC Security Policies)

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Contingency Planning and Business Recovery Program
IT System and Data Sensitivity Classification

Requirement:

(Jan 1, 2010 Revisions)

Each [Agency Head](#) or [designated ISO](#) shall:

- Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system. (BIA process, Section B2)
- Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.(BIA process, Section B2)

Note: Data and systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e. Microsoft SharePoint, PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc.