
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management – *Data Breach Notification*

Data Breach Notification

Purpose:

To specify the notification requirements for agencies by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information. When unencrypted COV personally identifiable information (PII) is subject to a breach in security resulting in unauthorized disclosure, the data owning agency shall provide appropriate notice to affected individuals. This notice should occur without unreasonable delay as soon as verification of a breach is made, consistent with the investigative needs of both COV CIRT and law enforcement entities. The *IT Security Standard*, Section 9.5, given below provides more information on the notification requirements.

All of the following are industry best practices. Where electronic records or IT infrastructure are involved, the following are requirements that each agency shall adhere to. *Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended: (Jan 2010 Revision)*

Requirements: (Jan 2009 Revisions)

SVCC shall:

1. Identify all agency systems, processes, and logical and physical data storage locations (whether held by the agency or a third party) that contain Personally Identifiable Information (PII) which means *a combination of a first name, or first initial, last name* and any of the following:
 - a. Social Security Number
 - b. Drivers license or Identification card number
 - c. Financial account number, credit or debit card number *and/or the corresponding password, security, or access codes.*
 - d. Other personal identifying information, such as insurance data or date of birth.

2. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
 - a. Provide immediate notification to the agency of suspected breaches; and tapes, USB drives, SD cards, etc

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management – *Data Breach Notification*

- b. Allow the agency both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.

- 3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted **and/or unredacted Personal Information** by any mechanism, including, but not limited to:
 - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's
 - b. Theft or loss of physical hardcopy; or
 - c. Security compromise of any system.

If the unauthorized release includes data that will allow or facilitate the decryption of data, the entity must treat the data as it is unencrypted.
If a data custodian is the entity involved in the data breach they must alert the data owner so that the data owner can notify the affected individuals.

- 4. In the case, a computer is found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules.

The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #6, below.

- 5. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of Personal Information that was involved;
 - c. What actions have been taken to protect the individual's personal information from further unauthorized disclosure;
 - d. What, if anything, the agency will do to assist affected individuals, including contact information **telephone number, if one exists, and additional contact information for more information and assistance;** and
 - e. What actions the agency recommends that the individual take.
Recommended should be in addition to monitoring the affected parties credit report and reviewing their account statements.

- 6. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. **Written notice to the last known postal address in the records of the individual or entity.**

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management – *Data Breach Notification*

- b. Telephone Notice
- c. Electronic notice
- d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice.

Substitute notice consists of all of the following:

- i. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
- ii. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
- iii. Notice to major statewide media.

7. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to section E. of Code of Virginia, §18.2-186.6, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. §1681(a)(p), of the timing, distribution, and content of the notice.

8. Not provide notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

9. Provide notice to the OAG if unencrypted and/or unredacted personal information is exposed. Personal information is considered redacted if the following applies to the exposed information:

- a. Five digits of a SSN are visible.
- b. The last four digits of a driver's license number or state identification card are visible.
- c. The last four digits of an account number are visible.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management – *Data Breach Notification*

Information Technology Security Standard COV ITRM Standard SEC501-01
Date: July 24, 2008 (Revision 4)

The individual Business Units at SVCC will be responsible for satisfying all the requirements of the *IT Security Standard ITRM SEC501-01*, section 9.5, Data Breach Notification, as given above. The System and or Data Owners for each Business Unit will be responsible for the identification, resolution, and documentation of all compliance issues as given in the standard.

The Business Units for SVCC are as follows:

1. Academic & Student Affairs
2. Administrative and Facilities Management
3. Adult Education
4. Dual Enrollment
5. Enrollment Management
6. Financial Aid
7. Information Technology
8. Institutional Advancement
9. Institutional Effectiveness
10. Library, Learning Resources
11. Middle College
12. Off Campus Instruction
13. President's Office
14. Student Services
15. Southern Virginia Higher Education Center
15. Workforce Development & Continuing Education