



## SENSITIVE DATA DEFINITION

SEC 501 defines "sensitive data" as follows:

*Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. Agencies must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits.*

As defined, information is deemed sensitive based on the following three criteria:

- Confidentiality - which addresses sensitivity to unauthorized disclosure.
- Integrity - which addresses sensitivity to unauthorized modification.
- Availability - which addresses sensitivity to outages.

It is in the best interest of the Virginia Community College System to ensure that data being collected, maintained, or accessed is protected. To ensure SEC501 standards are met, it is imperative that VCCS define sensitive information in a consistent manner across all 23 colleges. What follows is a synopsis of data that should be considered sensitive, and which must be protected. Also included is a list of items which are NOT sensitive, and a discussion of the items covered by FERPA. The definition provided is not all inclusive, but provides guidelines for colleges and personnel to follow.

PLEASE NOTE: This document is a general definition of sensitive data, and does not relieve colleges of the responsibility to evaluate their data based on high, moderate, and low levels of the confidentiality, integrity and availability criteria defined by SEC501.

### ***The following information/data is considered "Sensitive Information"***

- Items covered by FERPA (more on this below).
- Third Party Confidential information (both sent and received).
- Personally Identifiable Information (anything that could be used to identify you) as covered by the Government Data Collection & Dissemination Practices Act. *Note: Exceptions can be made by providing notice that information will be distributed (such as in a student handbook).*
- Financial Information as protected by the PCI Security Standard; or when integrity, confidentiality, and/or availability are an issue.
- Chancellor's or president's working papers or correspondence used for his/her own deliberative purposes and not otherwise open to the public.
- Electronic data covered by Attorney Client privilege.

*Other types of information should be discussed with the College CIO to determine the appropriate security level and how that information should be classified. If there are concerns and potential legal issues, the CIO should contact legal counsel for further interpretation before action is taken. This step will avoid a potential interruption in academic procedures.*

### ***The following information/data is NOT considered "Sensitive Information"***

- Financial Information - when integrity, confidentiality, and/or availability are not an issue.
- Directory Information - unless students opt out of having the information released.

**FERPA covers/does not cover the following:**

- FERPA covers educational records.
- FERPA covers those things “maintained” by the institution directly related to the student (such as SIS).
- FERPA covers the “official grade” for students, which is the FINAL grade, as stored in SIS. *The VCCS Policy Manual requires faculty to record a final grade (and a mid-term grade, if desired), but does not require the use of a gradebook. Based on policy, the only grade required, and thus the only grade protected, will be the final grade. All grades should be kept secure by the faculty member, but they would not be considered sensitive information.*
- FERPA does not cover directory information - including name, address, phone, email, place of birth, major, honors, degrees, and awards - unless the student opts out.
- FERPA does not cover information kept for the individual maker that is not intended to be shared (advisor's notes, gradebook information, etc). *If more than the individual maker has access to the information, then it is no longer exempted by FERPA.*
- FERPA does not cover records and/or test results for persons prior to their enrollment.

Faculty should take reasonable precautions to protect all student grades and gradebooks to maintain the integrity of the information. It is recommended that electronic gradebooks be stored on the network server, especially after the class ends.

FERPA violations come from a pattern or practice of releasing information. Serious violations could result in a loss of federal funding.

**POTENTIAL ISSUES with Vendors**

Publishers/Online Content

- Many publishers provide “online content” for free - some embedded into Blackboard, other available via website with a code from textbook.
- Students sign or approve a waiver/license agreement and are granted access to course material. Whether the agreement is between the students and the publisher, or the college and the publisher is determined as follows:
  - If the online content is OPTIONAL for the course, the student is consenting for the publisher to have their information; therefore the agreement is between the student and the publisher.
  - If the online content is a REQUIRED component, then the college is consenting for the publisher to have the information; therefore the agreement is between the college and the publisher.
- Faculty members should be aware of the type of information publishers will be asking for from the students, and ensure that it does not include sensitive information. *If the publisher will be collecting any type of sensitive information – THE COLLEGE CIO SHOULD BE CONTACTED IMMEDIATELY to determine whether a non-disclosure agreement is required.*
- Faculty members should never enter into a contract for the institution.

All Vendors

A vendor who stores sensitive information (as defined by VCCS) on their system, must keep that data confidential, and destroy information after it is no longer necessary. Vendors should sign a Non-Disclosure Agreement to ensure that this is part of the contract.

*If in doubt about a non-disclosure issue, contact the College CIO to determine the appropriate security level and whether a non-disclosure agreement is required. If there are concerns and potential legal issues, the CIO should contact legal counsel for further interpretation before action is taken.*