Virginia's Community Colleges Information Technology

Information Security Guideline

8.2.1 - Asset Management

Information Classification

Classification guidelines

Version: 2.1
Status: Revised – 2018-09-14
Contact: Chief Information Security Officer

Control

Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to VCCS.

Implementation Guidance

Requirement:
Classifications and associated protective controls for information should consider the business needs for sharing or restricting information and the business impacts associated with such needs.

Classification guidelines should include a naming/classification scheme for initial classification and reclassification over time; in accordance with the access control policy defined in VCCS IT Security Standard 9-1 Business Requirement for Access Control §§ 9.1.1 Access Control Policy.

It is the asset owner's responsibility (see VCCS IT Security Standard 8.1 Responsibility for Assets §§8.1.2 Ownership of Assets) to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. The classification process will consider the aggregation effect mentioned in VCCS IT Security Standard 8.3 Media Handling §§8.3.2 Disposal of Media.

Data will be classified as "Sensitive Information", "Private Information", or "Public Information" according to the protection requirements established by federal or state law, by the value (cost) to recover or replace the data, by the confidentiality of the data, by the integrity of the data, or by the critical need for data availability. The starting point for determining data protection requirements is the applicability of federal and state law and regulations governing data protection. The VCCS Business Impact Analysis and data collected about primary business

functions for each business unit must also be taken into consideration when determining the protection requirements for data. The value of data can be determined by assessing the impact to the VCCS if the data associated with a business requirement is lost or destroyed. Business functions that process, transfer, manage, or store sensitive data identify information systems that must be protected based on data confidentiality, integrity, or availability. The maximum tolerable downtime for an information system is one factor used to determine the criticality of the data to the VCCS.

Sensitive Data Definition

The VCCS has adopted the following definition of sensitive data as:

> "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."

For all data types, the sensitivity of the data due to loss of confidentiality, data integrity, or availability can be assessed according to the impact criteria in the following table:

Loss of:	**May result in:**
Confidentiality	System and data confidentiality refers to the protection of information from unauthorized access or 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.
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 essential IT system is unavailable to its end users, the organization's mission may be impacted. 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
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.
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.
Low - May result in the loss of some tangible assets or resources or may affect mission, reputation, or interest.

Note: A system/data should be considered sensitive if any of the three criteria contain a moderate or high rating. Sensitive information systems should always be protected at the highest possible level as necessary to maintain data confidentiality, integrity, or availability.

DATA CLASSIFICATIONS:

SENSITIVE INFORMATION

The following data is classified as Sensitive Information:

- **Student education records** as governed by the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).
- **Personally Identifiable Information** (anything that could be used to identify an individual) as governed by the Government Data Collection & Dissemination Practices Act (Code of Virginia Title 2.2 Chap. 38). Note: Limited PII disclosure **is allowed** through exceptions provided under FERPA regulations.
- **Third Party Confidential information** (both sent and received).
- **Federal Tax Information** entrusted to the college by the Internal Revenue Services or other tax return or financial data (FAFSA) furnished to the college by a student or parent.
- **Financial Information** as protected by the Payment Card Industry Data Security Standard (PCI DSS) or account information with a financial institution of any person or agency of the Virginia Community College System.
- **Contract Information** declared to be proprietary or while under negotiation prior to award as governed by the Virginia Public Procurement Act.
- **The Chancellor's or president's working papers** or correspondence used for his/her own deliberative purposes and not otherwise open to the public.
- **Public Safety Records** as defined and governed by § 2.2-3705.2 of the Virginia Freedom of Information Act.
- **Administrative Investigation Records** as defined and governed by § 2.2-3705.3 of the Virginia Freedom of Information Act.
- **Educational Records** as defined and governed by § 2.2-3705.4 of the Virginia Freedom of Information Act.
- **Law-enforcement and criminal records** as defined and governed by § 2.2-3706 of the Virginia Freedom of Information Act.
- **All data covered by Attorney Client privilege.**

Data must be classified as Sensitive Information when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to VCCS or the colleges. The

highest level of security controls must be applied to Sensitive Information. Sensitive Information is not necessarily confidential data but can be data whose integrity or availability require that it be protected from unauthorized alteration or loss.

PRIVATE INFORMATION

Data must be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to VCCS or the colleges. By default, all Institutional Data that is not explicitly classified as Sensitive or Public data should be treated as Private data. A reasonable level of security controls must be applied to Private data.

PUBLIC INFORMATION

Data must be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the VCCS or the colleges. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Additional Information:

Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels.

The Family Educational Rights and Privacy Act (FERPA) CFR Title 34 Part 99

The privacy and disclosure of student educational records is governed by the provisions of FERPA which restricts disclosure of educational records to eligible students (18 years and older) unless prior consent is obtained or if disclosed in accordance with exceptions to the Act.

FERPA requirements protect the following information from disclosure:

- Student educational records.
- Records "maintained" by the institution directly related to the student (such as SIS records).

FERPA allows exceptions to the disclosure restrictions including:

- The release of directory information (as defined in this document) is permitted with prior notice and implicit consent - including student name, place of birth, major, honors, degrees, and awards and other such information under certain conditions unless the student opts out.
- Allowable use of a student ID number or other unique personal identifier to be used by a student to access or communicate using electronic systems when such access or use requires one or more additional factors to authenticate the student's identity.
- Allowable use of a student ID number or other unique personal identifier displayed on a student ID badge if the identifier cannot be used to gain access to education records

except when used in conjunction with one or more factors to authenticate the student's identity.

- Information kept for the individual maker that is not intended to be shared (advisor's notes, gradebook information, etc.) are not considered educational records unless other persons also have access to the information, then it is no longer exempted by FERPA protections against disclosure.
- Grades on peer-graded papers and assignments are not considered educational records until they are collected and recorded by the course instructor.
- Records and/or test results for persons prior to their enrollment and attendance of the first day of class are not protected student records.
- Disclosure to a school official or agency acting in this capacity when used to for a legitimate educational purpose.
- Disclosure on behalf of the educational institution to facilitate predictive testing, administer student aid programs, or improve instruction. Such disclosure needs to be recorded and the receiving entity may not re-disclose such information or use it for any other unintended purposes.
- Disclosure to federal or state educational authorities for the purpose of audit or evaluation of a federal or state sponsored program or to enforce compliance with educational program requirements. Such disclosure needs to be recorded and the receiving entity may not re-disclose such information without written consent and agreement of the educational institution.

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.

Personally Identifiable Information

Personally identifiable information means information that can be used to uniquely identify an individual when used alone or in combination with other personal information.

All information that (i) describes, locates or indexes anything about an individual including, but not limited to, his social security number, driver's license number, agency-issued identification number, student identification number, real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or (ii) affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

"Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information.

Student identification numbers may be exempted from classification as sensitive data if declared to be "Directory Information" intended to be published with notice and consent given according to the requirements of FERPA **§99.37**.

Directory Information

Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

> Directory information may include, but is not limited to, the student's name; photograph; place of birth; major field of study; enrollment status (e.g., full-time, part-time, inactive); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

Directory information may be disclosed in accordance with federal and state law and regulations, provided that the school has given notice to the parent or eligible student of (i) the types of information that the school has designated as directory information; (ii) the right of the parent or eligible student to refuse the designation of any or all of the types of information about the student as directory information, and (iii) the period of time within which the parent or eligible student must notify the school in writing that he does not want any or all of the types of information about the student designated as directory information.

No school shall disclose the address, telephone number, or email address of a student unless the parent or eligible student has ***affirmatively consented in writing*** to such disclosure.

Social Security Numbers (SSN) and Date of Birth (DOB) ***are never*** considered to be directory information and must be protected as restricted data at all times.

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.

Potential Issues with Vendors

Publishers/Online Content

- Many publishers provide "online content" for free - some embedded into the Learning Management System, other content 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 ISO should be contacted IMMEDIATELY to determine whether a non-disclosure agreement is required.

- Faculty members must never enter into a contract for the institution.

All sensitive/confidential data must be encrypted if it is being transmitted in any form over public transmission lines, with the encryption methodology to be agreed upon between the vendor and the data owner. The requirements are governed by the VCCS Information Security Standard 10.1 Cryptographic Controls and related procedures. The procedures are not available for public viewing. Further information on requirements can be provided, if requested.

A vendor who stores sensitive information with respect to confidentiality (as defined by VCCS) on their system, must keep that data confidential, and destroy information after it is no longer necessary. Vendors must 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.

Other Information

Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense.

Considering documents with similar security requirements together when assigning classification levels might help to simplify the classification task.

In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

REVISION HISTORY

Date	Version	Reviewer	List of Changes
2013-02-23	1.0	CISO	Revised draft to final
2014-01-28	1.1	S. Bumpas	Added sensitive data definition, types of sensitive data, distinctions between sensitive/non-sensitive data, and vendor considerations. Formatting changes, added revision page
2016-11-07	2.0	J. Skinker	Renumbered the section to move from Section 7.2.1 to Section 8.2.1 as part of the Standards realignment with ISO 27002:2013. Made various formatting changes.
2018-09-14	2.1	J. Skinker	Revised Directory Information allowable data. Added new Data Classifications. Added new Sensitive Data definitions. Added clarifications for FERPA allowable disclosures.

Final Approval

Date	Name	Position	Signature