DATA CLASSIFICATION

DATA BRIEF

The following data classifications apply to the SBCTC Data Warehouse. Data in the SBCTC Data Warehouse is considered "data at rest".

The Office of the Chief Information Officer (OCIO) data classification definitions are shown below and are considered the minimum acceptable definitions. The SBCTC's definitions strive to be equal to or more secure than those of the OCIO.

Guiding Principles

- Any data set that includes multiple levels of classifications automatically assumes the highest level of classification for the entire data set, regardless of individual data element classification.
- Information that can be derived with Public Directory information alone is also considered Category 2 data unless otherwise noted in the field details (e.g. county can be derived from address; age can be derived from birthdate, etc…).

Category 1: Public Information

OCIO Definition: *Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.*

SBCTC Definition: SBCTC does not consider any Data Warehouse data to be category 1. SBCTC does not release data to the public unless specifically requested. The release of public information is reserved for the college's discretion based upon their FERPA directory information policies.

Category 2: Sensitive Information

OCIO Definition: *Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to public unless specifically requested.*

SBCTC Definition: Student related information that is considered "directory information" under FERPA and is generally not considered harmful or to be an invasion of privacy if released. This information can be disclosed to outside organizations with the student's prior consent. This is information that would be released during a public records request of Data Warehouse data. Directory information includes:

- Student name
- Most recent educational agency or institution attended *(College Code and Name)*
- Dates of attendance *(YRQ)*
- Degrees, honors, and awards received *(Exit Code and Exit Code Description)*

Note: Information that can be derived with Public Directory information alone is also considered Public Directory Information unless otherwise noted in the field details (e.g. county can be derived from address; age can be derived from birthdate, etc…).

SBCTC also considers course and program information not associated directly to a student as category 2 information. This includes:

- Department and Course Number
- Course Title
- Course Intent
- Program Code (EPC)
- Program Title

Category 3: Confidential Information

OCIO Definition: *Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:*

a. Personal information about individuals, regardless of how that information is obtained.
b. Information concerning employee personnel records.
c. Information regarding IT infrastructure and security of computer and telecommunications systems.

SBCTC Definition: Enrollment information protected under FERPA, personnel and financial data. Category 3 includes all data elements except those explicitly stated in categories 2 and 4. Category 3 data is not distributed unless governed by a contract or data sharing agreement. This information is protected due to:

a. Sensitivity - Information which must be protected due to proprietary, ethical, contractual or privacy considerations.
b. Legal Obligations - Information for which disclosure to persons outside of the SBCTC may be governed by specific standards and controls designed to protect the information such as FERPA.
c. Moderate risk - Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the SBCTC or college reputation, violate an individual's privacy rights, or make legal action necessary.

This information includes but is not limited to:

- Student Identification Numbers
- Grades
- Courses taken
- Test Scores
- Educational services received
- Bio-demographics (e.g. race, gender, family status, employment status)
- All personnel data including salaries
- All financial data

Category 4: Confidential Information Requiring Special Handling

OCIO Definition: *Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:*

a. *Especially strict handling requirements are dictated, such as by statutes, regulations or agreements.*
b. *Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.*

SBCTC Definition: Highly confidential data that is exempt from disclosure under applicable state and federal laws such as personally identifiable data protected under FERPA. Category 4 data is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to SBCTC or colleges, students, employees or customers. This information has limited use per specific state and federal laws. This information includes:

- Social Security Number (SSN)
- Health Limitations

Category 4 data elements may only be disclosed to educational authorities in Washington State. Per RCW 43.41, educational authorities include the community and technical colleges, State Board for Community and Technical Colleges, Office of Financial Management's Education Research and Data Center, the Workforce Training and Education Coordinating Board and the Washington State Student Achievement Council. A student's social security number may be shared with the Washington Employment Security Department for the purpose of obtaining outcomes related employment data only with the consent of the student and under specific data sharing agreements.

Other examples, though not available in the data warehouse, include but are not limited to:

- Credit card numbers
- Tax ID
- Driver's license number
- Bank account or debit card information
- Electronic or digitized signatures