

SBCTC DATA CLASSIFICATIONS

Know It. Protect It. Use It Responsibly.

These guidelines help Washington's community and technical colleges classify, protect and handle data consistently. All data, whether in ctcLink or another system, must be managed according to its classification.

THE FOUR DATA CLASSIFICATION CATEGORIES

Important: When data categories are combined, protect the entire dataset at the highest classification level.

[CLASSIFICATION WORKBOOK](#)

Operational reference for classifying specific ctcLink records and fields.

[CLASSIFICATION GUIDELINES](#)

Framework, definitions, criteria and handling requirements.

1 PUBLIC INFORMATION

Information that can be released publicly.

- Does not identify individuals (students, employees, customers, or vendors).
- No encryption required at rest or in transit.
- Review for accuracy and integrity before sharing.

2 SENSITIVE INFORMATION

Official-use information that may include PII.

- Examples: student directory information, general employee information.
- Encryption not required by standard.
- Encryption at rest is recommended as best practice.

3 CONFIDENTIAL INFORMATION

Information protected from disclosure by law.

- Examples: student enrollment records, protected employee information, nonpublic financial information tied to an individual that describes the services rendered, FERPA-blocked information.
- Must be encrypted at rest and in transit.
- Access limited to authorized individuals.

4 CONFIDENTIAL — SPECIAL HANDLING

Highly sensitive data with strict legal, regulatory, or contractual requirements.

- Examples: Social Security numbers, driver's license numbers, passport numbers, financial account details, health data, authentication credentials.
- Encryption required at rest and in transit.
- Access controls, monitoring, and audit logging required.
- Only share when necessary and legally justified

KEY POINTS TO REMEMBER

- Classify all data based on the highest sensitivity level when combined.
- Follow the handling requirements for each classification category.
- Limit access to those with a legitimate business need.
- Protect data through encryption, secure storage, and safe sharing.
- Know the laws and policies that apply to the data you handle.

NEED HELP CLASSIFYING?

Use the decision trees in the [Guidelines](#)

- Student Data—page 12
- Employee Data—page 13
- Financial Data—page 14

TERMS TO KNOW

- **PII:** Information that can identify an individual, such as a name, email or Social Security number.
- **NPI:** Non-public financial information
- **FERPA Directory Information:** Student information that may be released unless the student opts out.

HAVE QUESTIONS?

Consult your IT department. Your IT team is your partner in protecting our data and our students.