Green River Data Handling Guidelines

GRC classifies data (college information) per the SBCTC and WA State OCIO guidelines.

All GRC Data must be stored either physically on a GRC campus or digitally on GRC CTR (i.e., resources provided by GRC either directly or through agreements with contracted entities). GRC Data must not be stored off-campus (other than during approved and temporary travel), on personal equipment or in non-GRC provided or contracted solutions.

Category 2 and higher data requires specific care be taken when transmitting or storing and should not be stored on any non-GRC owned equipment without a signed confidentiality and data sharing agreement. Category 2 and higher data is discoverable.

Per the GRC IT Security Policy:

4.1. Data Classification

GRC classifies data into categories based on the sensitivity of the data. GRC data classifications must translate to or include the following classification categories:

1. Category 1 – Public Information

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.

Public Information data includes the mission/vision/values of an agency, information related to obtaining services, staff phone numbers, work e-mail addresses, budget information, and FERPA "directory information" designated at Green River College as FERPA information at level 1.

Electronic transfer of data in this classification is not restricted.

2. Category 2 – Sensitive Information

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

Sensitive data should not be transferred outside the GRC network electronically unless on password protected media. You must be specifically authorized to transfer such data outside the agency. Transfer inside the GRC network is allowed.

Specific examples include, but are not limited to:

- Data Warehouse data unless that data falls under a Category 3 or 4 classification
- Student Directory Information as per FERPA regulations can be disclosed to outside organizations with the student's prior consent or released during a public records request of Data Warehouse data.
- Certain personnel records – e.g., misconduct records subject to public disclosure
- Public Employee Financial information, but not salaries as this is public information

- Directory Information includes:
    - Student name
    - Student birthplace and birthdate
    - Student address
    - Student telephone number
    - Student e-mail address
    - Major field of study (EPC)Dates of attendance (YRQ)
    - Degrees and awards received
    - Photograph
    - Participation in officially recognized activities or sports
    - Height and weight of athletes
    - Most recent educational agency or institution attended
    - Other similar information
- Directory information does NOT include:
    - Social security number
    - Student identification number
    - Race
    - Ethnicity
    - Nationality
    - Gender
    - Class schedule
    - Course and Program information not tied directly to a student, such as:
        - Department and Course Number
        - Course Title
        - Course Intent
        - Program Code (EPC)
        - Program Title

3. Category 3 – Confidential Information

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

- Personal information about individuals, regardless of how that information is obtained such as home address, phone number, and personal e-mail address
- Information in employee personnel records including evaluations
- Information regarding IT infrastructure and security of computer and telecommunications systems
- All financial data not included in the Public Employee Financial Information data
- Personal network user information (e.g., usernames and passwords)
- Enrollment information protected under FERPA such as:
    - Student Information Numbers (SIDs)
    - Grades
    - Courses taken
    - Test scores

- Educational services received

This category of data can be transferred internally, with appropriate care – e.g., marked in e-mail as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency and there must be a signed confidentiality agreement with that individual or company prior to sending the information.

SBCTC Definition of Category 3 Data:

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 and individual's privacy rights, or make legal action necessary.*

This information includes but is not limited to:

- *Student Identification Numbers (SID)*
- *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*

Confidential Information data includes personal network user information, data related to IT security, employee and student personal information such as ID number, home address, phone number, personal email address, including information designated as Green River College FERPA levels 2 & 3.

This category of data can be transferred internally, with appropriate care – e.g., marked in email as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the college via password protected or encrypted media. You must be specifically authorized to transfer such data outside the college.

Specific examples include, but are not limited to:

- *Personnel records. – e.g., Evaluations*
- *Employee personal Information – e.g., home address, home email, home phone*

Note: Student email (personal or Green River Student Email) is not considered an internal transfer and sensitive data must be sent via encrypted email.

4. Category 4 – Confidential Information Requiring Special Handling

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

- Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements (such as FERPA, HIPAA, or PCI-DSS)
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions

Confidential Information Requiring Special Handling includes employee or student information such as social security number, date of birth, etc., and information designated as Green River College FERPA level 4.

Specific examples include, but are not limited to:

- Banking/Financial Account information
- Records protected by PCI-DSS such as Credit Card Numbers
- Employee and Student Social Security Numbers
- Date of birth
- Student Identification Numbers (SID)
- Academic records of matriculated students
- Educational records protected by FERPA
- Medical records protected by HIPAA
- Medical Records, including psychological/counseling records

This category of data can be transferred internally, with appropriate care – e.g., marked in e-mail as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency.