DATA GOVERNANCE, ACCESSIBILITY, & CLASSIFICATION

Policy Number: CU-IT-77

SECTION 1. GENERAL

1.1 Scope: This policy applies to all students, employees, officers, contractors, sub-contractors, grantees, grantors, and any person or entity internal or external to the University accessing, controlling, requesting, or otherwise attempting to utilize institutional data.

1.2 Authority: W. Va. Code § 18B-1-6; 133 C.S.R. 4, Rules and Administrative Procedures

1.3 Effective Date:

1.4 Purpose: The purpose of this Policy is to establish an effective governing framework for the management, access, and use of institutional data consistent with applicable state laws and federal regulations. Concord University recognizes the dual demands of maintaining transparent, diverse, and robust data in support of its teaching, research, and strategic goals while protecting the privacy of its students, prospective students, employees, and prospective employees. Concord University views effective data governance as critical to achieving its mission, enhancing decision-making processes, and ensuring the privacy and security of sensitive data.

SECTION 2. POLICY

2.1 Data Governance Framework: It is the policy of Concord University to establish and maintain stringent actions, structures, and classification schemes necessary for the protection, access, and use of institutional data by any and all parties internal or external to the institution.

2.2 Data Ownership and Stewardship: The institution shall establish and maintain designated internal data owners and stewards of data, as defined below, who are responsible for the quality, integrity, and appropriate use of data.

2.3 Data Lifecycle: The University shall manage institutional data throughout the data's lifecycle, including its creation, storage, transmission, and disposal in accordance with institutional policies, procedures, and legal requirements.

2.4 Data Classification: Institutional data shall be classified based on its privacy sensitivity, with categories such as Public, Internal Use, and Restricted.

2.5 Data Requests, External Parties: The University shall establish and maintain auditable controls for approving, denying, and monitoring access to institutional data from external parties.

a. The University shall ensure all requests for institutional data from parties, persons, or entities external to the University are acquired, maintained, and recorded in writing electronically through the Office of Institutional Research.

b. The University shall ensure, upon receipt of requests and inquires for institutional data from persons or entities external to the University, that the request or inquiry is reviewed regarding:

i. the potential risks of specified data sharing necessary to satisfy the request,
ii. the privacy of any person-level information contained within or represented by such institutional data necessary to satisfy the request; and
iii. the purpose, scope, and duration for which the data is requested.

c. The University shall ensure all external data requests are approved by a Data Owner and Cabinet-level official prior to the dissemination of requested institutional data.

d. The University reserves the right to require a signed data sharing agreement that defines the terms, conditions, restrictions, transmission, use, and destruction of data for any approved external data request which may contain personally identifiable information or data considered protected under any Federal or State law.

2.6 Data Requests, Internal Parties: The University shall establish and maintain auditable controls for approving, denying, and monitoring requests for access to institutional data from internal parties.

a. The University shall ensure all requests and inquires for institutional data from internal parties are acquired, maintained, and recorded in writing electronically

through the Office of Institutional Research or other institutional offices or officials designated in writing electronically by the University as a Data Owner.

b. The University shall ensure, upon receipt of requests and inquires for institutional data from internal parties, that the request meets the Legitimate Educational Interest standard set forth in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232(g); 34 CFR Part 99.

    i. The internal party must be a school official who has a legitimate educational interest in the data, which interest may include, but is not limited to:
        1. Performing a task that is specified in his/her position description.
        2. Performing a task related to a student's education or disciplinary matter.
        3. Providing a service or benefit related to the student or student's family.
        4. Maintaining safety and security on campus.

c. For internal parties requesting institutional data for the purpose of acquiring a Federal, State, or Local grant or maintaining compliance with a Federal, State, or Local grant, Section 2.6 of this Policy governs.

d. For internal parties requesting data on behalf of or for use by an external party, Section 2.5 of this Policy shall govern.

2.7 Data Access Controls: Access to institutional data containing person-level data will be granted by Data Owners and based on role-specific permissions and the principle of least privilege.

2.8 Data Encryption: Institutional data containing person-level data or data protected by any Federal or State law shall be encrypted during transmission and storage using industry-standard encryption protocols.

2.9 Data Retention and Destruction: The University shall securely retain and destroy institutional data in accordance with legal and regulatory requirements and any policy promulgated by the University.

2.10 Enforcement: The University reserves the right to take any and all measures necessary to protect the quality, integrity, and appropriate use of institutional data, including through established disciplinary processes, legal action, and referral to law enforcement.

2.11 Training and Education: The University shall provide data governance training annually to all employees of the University and establish a public website of resources that include information on data governance policies, procedures, and practices of the University.

2.12 Publicly available data: The University shall establish, maintain, and update within a reasonable timeframe a public website containing or otherwise linking to accurate, verified aggregate data which represents multiple aspects of its student populations and academic programs. Data must be presented in plain language with clear data definitions and the institution's methodology for compiling such data, including any student populations excluded from the data, disclosed in an accessible format. Data made available in aggregate form must reflect at minimum:

a. Enrollment
b. Retention
c. Completions
d. Required state licensure exam pass data
e. Student outcomes data after transfer or graduation (such as continuing education, job placement and estimated earnings)
f. Other data required by any outside accreditor, as applicable

SECTION 3. DEFINITIONS

3.1 Institutional Data: Person-level or aggregate information created, collected, maintained, transmitted or recorded by or for the University that is:

a. Subject to a legal obligation requiring the University to responsibly manage, report, or protect the data.
b. Relevant to planning, managing, organizing, operating, documenting, staffing, assessing, or auditing one or more functions of the University.
c. Used to derive any data aggregate or person-level from any of the above.

3.2 External Parties: Any person, company, or entity not employed by or doing business for or on behalf of the University for which a signed contract or other written formal agreement is on record at Concord University.

3.3 Internal Parties: Faculty, staff, students, and employees of Concord University, including contractors and grantees.

3.4 Data Owner: An employee of the University responsible for the definition, usage, and access rights of designated institutional data. This role is assigned by the University for specific data sets or systems.

3.5 Data Steward: An employee of the University responsible for the day-to-day usage, maintenance, and quality of institutional data to which they are granted access.

3.6 Principle of Least Privilege: The minimum level of access to institutional data necessary to perform a defined job function.

3.7 Person-level Data: An individual data point or set of data points reflecting information about a singular person.

3.8 Aggregate Data: A data point or set of data points reflecting information about multiple persons.

SECTION 4. AMENDMENTS

This Policy may be amended to change names, titles, links to information, grammar, and spelling without going through the rulemaking process.

Federal and State laws, rules and regulations change. The Board may modify any portion of this policy to conform the College's practices with such changes. Subject to the institution's rulemaking policy, the institution will change this policy to conform to the most current laws and regulations within a reasonable time of discovering the change.

APPROVAL

Intent to Plan Approved: November 14, 2023
Approved by the Board of Governors: April 16, 2024