WESTERN NEBRASKA COMMUNITY COLLEGE

President's Procedure

TITLE:	Data Governance
DIVISION:	General Institutional
CATEGORY:	Records/Information
REFERENCE:	Data Integrity Board Policy BP-413 Confidentiality of Employee Records Board Policy BP-551 Confidentiality of Student Records Board Policy BP-410 Conflict of Interest and Code of Ethics Board Policy BP-810 Gramm-Leach-Bliley Student Financial Board Policy Information Security Program Board Policy BP-701 Records Management, Retention and Disposition Board Policy
NUMBER:	PP-702
DATE OF APPROVAL:	2019
APPROVAL:	John Harms, Interim President

Western Nebraska Community College (WNCC) is committed to the responsible collection, dissemination, and utilization of data in an ethical and compliant manner. The integrity and accuracy of all the information WNCC maintains and shares is critical to the success and measurement of institutional effectiveness. Therefore, there shall be:

- Standards for collecting, cross-checking, and verifying all data elements.
- Procedures for submitting all data, including required reviews and approvals.
- Certification by Data Stewards of integrity and accuracy of all data, both prior to and after submission.
- Mechanisms for questioning or raising concerns, directly or anonymously, about the integrity or accuracy of data.
- Standards for maintenance, storage, and retrieval of all data elements.

This procedure governs all aspects of the College. All WNCC employees who use data, regardless of the form of storage or presentation, shall abide by this procedure. All senior administrators have the responsibility to understand and implement this procedure, including, as necessary, the adoption of specific procedures for their respective areas in furtherance of and in accordance to this procedure.

Definitions

Data Classification: See Appendix A

Data Element: A single data item (i.e., a last name is a data element).

Data Dictionary: A reference tool, which provides a description of all the core institutional data elements.

Data Dissemination: The distribution of data to either internal or external stakeholders. Included in dissemination is the sending of data to external entities including vendors that provide services for WNCC.

Data Integrity: The qualities of reliability and accuracy of data values that permit the institution to have dependable data on which to make plans, projections and decisions. Data integrity contributes to the efficient operation of the institution by supporting quality customer service to students, faculty, and employees and helping the institution remain competitive.

Data Integration: The ability of data to be assimilated across information systems is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Data Model: A diagrammatic representation of the objects and their properties that are needed within an organization to accomplish its mission. Sometimes represented as an ER (entity-relationship) diagram or a data flow diagram.

Data Steward: Managers of functional areas of Colleague (typically at the level of Registrar, Director of Admissions, Director of Human Resources, etc.) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data stewards are responsible for making security decisions regarding access to the data under their purview.

Data Value: The set of values that each data element can have. For example: numeric or alpha for academic departments (i.e. ACCT or ENGL).

Institutional Data: The data elements that are aggregated into metrics relevant to operations, planning, or management of any unit at WNCC; that are reported to the WCCA Board of Governors, federal, and state organizations; generally referenced or required for use by more than one organizational unit; or included in official administrative reporting.

Procedure

Institutional data are assets maintained to support the College's mission of "…enriching lives, invigorating communities, creating futures." To support effective and innovative management, institutional data must be accessible, correctly represent the information intended, and be easily integrated across WNCC's information systems to support the organization's strategic plans. The WNCC executive leadership team recognizes the value-added benefits of being able to aggregate information across multiple complex systems and business processes that enable WNCC to fulfill its mission.

Procedures shall be strictly adhered to for:

Data Access

Employees shall have the correct access (read-only or write) to data elements as required by the functionality of that position. Any employee or non-employee denied access may appeal the denial to the Vice President for Administrative Services. Escalation to the WNCC President should only be pursued if the Vice President's decision is being appealed.

Data Usage

Personnel will have applicable access to data only as required for the performance of the job function; data will not be used for personal gain. Data usage shall be either for *update* or *dissemination*.

Update

Authority to update data shall be granted by the appropriate Data Steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with WNCC's desire to provide excellent service to faculty, staff, students, and other constituents. Data Stewards shall ensure that adequate internal controls and/or change management procedures are in place to manage "updates" to key institutional data, their definitions and processes.

Dissemination

Dissemination of data must be controlled in accordance with the security practices set forth by the Data Stewards. Appropriate use must be considered before sensitive data are distributed. Unauthorized dissemination of data to either internal/external personnel is a violation of the Board Policy and this Presidential Procedure.

System-to-System Interfaces

System-to-System Interfaces are a standard practice to move data from one system to another and may be utilized in order to streamline processes that extend across systems and contribute to using data efficiently and effectively. The Enterprise Resource Planning (ERP) Governance Committee must approve such interfaces for such operational processes. The systems that exchange information fall into two broad categories:

- *Internal* – Systems that are implemented within the WNCC computer systems network. They can either be procured, procured but modified, or custom developed products.
- *External* – Systems that do not reside on a WNCC computer network. These systems are hosted by vendors and/or through sub-contracts managed by vendors.

Data Integrity

Processes or data systems shall be utilized to validate the integrity of the data and validate rules that ensure the highest level of data integrity are achieved and maintained. Validation rules within data systems may need to include reconciliation routines (checksums, hash totals, record counts) to ensure that software performance meets expected outcomes. Data verification programs that validate consistency and reasonableness of data shall be implemented to identify data tampering, errors, or omissions.

Enterprise Resource Planning (ERP) Governance Committee

The ERP Governance Committee is responsible for establishing data governance, protocols, standards, and guidelines for ensuring maximum value of WNCC data can be achieved.

The data governance structure includes sections on data access, usage, integrity, and integration. Adherence to the data governance guidelines shall:

- Establish appropriate responsibility for the management of institutional data as an institutional asset.

- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Improve the storage and security of the data, including confidentiality and protection from loss, utilizing a metadata repository.
- Improve the integrity of the data, resulting in greater accuracy, timeliness, and quality of information for decision-making.
- Establish standard definitions for key institutional data to promote data integrity and consistency.

The purpose of data governance is to develop institution-wide policies and procedures that ensure that WNCC data meet these objectives within and across the administrative or academic data systems. The function of applying protocols, standards, guidelines, and tools to manage the institution's information resources is termed data governance. Responsibility for the activities of data governance is shared among the roles listed below. Descriptions of roles and responsibilities below provide the framework of how data governance will be implemented and maintained.

Function

The ERP Governance Committee is the body responsible for developing and submitting to the Executive Sponsor for approval the data governance policy on data access, data usage, data integrity and integration, and data security; proposing prioritization of business intelligence work; ensuring that work plans are established and met; and reporting up to the Executive Sponsor on project status and seeking input on projects that have broad institutional implications related to business intelligence and data. Assignment of personnel to the key roles listed below requires consensus within the ERP Governance Committee.

Executive Sponsor

The Executive Sponsor is a senior WNCC official responsible for setting the overall prioritization for institutional business process redesign projects; communicating process transformation priorities across the institution; ensuring project resources are available and adequate to meet established time lines; bringing clarity whenever necessary to projects, processes, and data work; carrying proposed data governance policy forward for consideration and approval; and appointing members of institutional data governance committees. The Executive Sponsor will review and make initial decisions on policies presented by the ERP Governance Committee.

Membership

The Executive Sponsor is responsible for the ERP Governance Committee membership. Changes to the ERP Governance Committee membership must be nominated to the ERP Governance Committee. Upon approval, the Executive Sponsor will review and provide a final decision based on the recommendation.

Data Standards & Reporting Committee

The Data Standards & Reporting committee is a sub-committee of the ERP Governance Committee. This committee carries out protocols set by the ERP Governance Committee, addresses data quality and integrity, and sets forth data standardization and standard reporting practices into the institutional reporting environments.

- Membership – The ERP Governance Committee is responsible for the Data Standards & Reporting committee membership. Changes to the membership must be nominated to the ERP Governance Committee. The ERP Governance Committee will review and provide an approval decision based on the recommendation.

Revising this Procedure

If statutory provisions, regulatory guidance, or court interpretations change or conflict with this President's Procedure, the College retains the right to revise accordingly and for the changes to take effect immediately.

Appendix A

Appendix A

Data Classification

Level 1 – PUBLIC

Low risk if revealed to the public at large. Some controls need to be in place to prevent unauthorized or accidental modification or destruction.

Includes but not limited to:

- Newsletters
- Staff directory
- Course catalogs
- Annual reports

Level 2 – PRIVATE

Moderate risk of financial loss, public distrust, and/or legal trouble if unauthorized access, release, alteration, or destruction of this data occurs. By default, ALL College data should be treated data as private unless explicitly classified as public or protected. Reasonable levels of controls should be in place to protect this data.

Includes but not limited to:

- Security system information (Physical and System wide)
- College financial data
- Audit reports
- Email addresses that aren't public record

Level 3 – PROTECTED

Significant risk of financial loss, public distrust, and/or legal trouble if unauthorized access, release, alteration, or destruction of this data occurs. The highest level of controls should be in place to protect this data.

Includes but not limited to:

- PII (Personally Identifiable Information)
- Any combination of – full name, address, social security number, Colleague ID
- Passwords or PINs
- HIPAA (Health Insurance Portability and Accountability Act)
- ePHI (electronic Protected Health Information)
- FERPA (Family Educational Rights and Privacy Act)
- GLBA (Gramm-Leach-Bliley Act)
- PCI-DSS (Payment Card Industry – Data Security Standard)