Administrative Policy #: TBD

Title: Data Entry Standards

Effective Date: TBD

SECTION 1. PURPOSE & SCOPE

1.1. PURPOSE: The purpose of this policy is to establish institution-wide standards for the entry, modification, and validation of institutional data to ensure accuracy, consistency, security, and reliability across all university systems. High-quality data is essential for operations, compliance reporting, analytics, accreditation, and decision-making.

1.2. SCOPE: This policy applies to all institutional data entered into any university system, including but not limited to:

1.2.1. Enterprise Resource Planning (ERP) systems

1.2.1.1. Student Information Systems (SIS)

1.2.1.2. Human Resources (HR) and Payroll Systems

1.2.1.3. Finance and Accounting Systems

1.2.2. Customer Relationship Management (CRM) Platforms

1.2.3. Housing/Residence Hall systems

1.2.4. Card/Mobile Customer Access Systems

1.2.5. Learning Management Systems (LMS)

1.2.6. Research Administration Systems

1.2.7 Facilities, Security, and Auxiliary systems

1.2.8 College, Department, and other Miscellaneous Systems

SECTION 2. APPROVAL, DELEGATION & APPLICABILITY

2.1. AUTHORITY: The Chief Information Officer and Executive Director of Institutional Research & Effectiveness have authority to make decisions regarding this policy.

2.2. DELEGATION: Data Owners are responsible for the entry of data. Data Stewards are responsible for the validation of data and comprised of the Institutional Research

Divisions. Data Custodians are to monitor and modify the classifications of data and are comprised of the Information Technology Divisions.

2.3. APPLICABILITY: This policy applies to:

Individuals: All University faculty, staff, administrators, student employees, and other authorized users who access, enter, update, or use data in the system of record.

Systems: Any third-party or ancillary application that transmits data to, or receives data from, the system of record.

Units: All academic and administrative units are responsible for the accuracy, security, and maintenance of institutional data within their areas of operation. Students accessing the ERP are subject to applicable student use and data privacy policies but are not considered under the primary scope of this policy.

SECTION 3. DEFINITIONS *(Clarification of key terms and concepts used in the policy.)*

3.1 **Access Control:** Mechanisms and policies that determine who is allowed to access specific data or systems and under what conditions. Access control ensures that only authorized individuals can view or interact with sensitive or confidential information.

3.2 **Ancillary System:** Any third-party application, database, or tool that uses, stores or derives data from our ERP.

3.3 **ERP:** The University's Enterprise Resource Planning (ERP) system, which serves as the central student information system and repository for related academic and administrative data.

3.4 **Confidential Data:** Data that requires protection due to legal, regulatory, or contractual requirements. Disclosure of confidential data could result in legal, financial, or reputational harm. Examples include student records subject to the Family Educational Rights and Privacy Act (FERPA), employee data, and health-related information subject to Health Insurance Portability and Accountability Act (HIPAA).

3.5 **Data Anonymization:** The process of removing or modifying personal identifiers from data so that the data can no longer be linked to an individual, thereby reducing privacy risks.

3.6 **Data Classification**: The process of categorizing data based on its level of sensitivity, value, and legal or regulatory requirements. Data classification determines the handling, access control, storage, and disposal requirements for each type of data.

3.7 **Data Disposal:** The process of permanently deleting or destroying data when it is no longer required or has reached the end of its retention period. This can include secure deletion of electronic files or physical destruction of paper records.

3.8 **Data Integrity:** The accuracy, consistency, and reliability of data over its lifecycle. Ensuring data integrity means that the data is maintained without unauthorized modification and that it is trustworthy for decision-making.

3.9 **Data Masking:** A technique used to protect sensitive data by replacing it with fictional or scrambled data. This allows for the use of realistic data for testing or analysis purposes without exposing actual sensitive information.

3.10 **Data Owner:** An individual or department responsible for the creation, management, and protection of a specific dataset. Data owners are responsible for determining the classification level of the data they manage.

3.11 **Data Sensitivity:** A measure of how critical or private data is, determining the level of protection it needs. Sensitive data is typically defined by the potential impact to the University or individuals if the data is disclosed, altered, or destroyed in an unauthorized manner.

3.12 **Data Stewardship:** The responsibility for ensuring that data is properly managed, protected, and used according to institutional policies, legal requirements, and ethical standards. Data stewards are typically the individuals or departments responsible for specific data sets.

3.13 **Data User:** Any individual who accesses, processes, or handles University data, including faculty, staff, students, contractors, or third-party partners. Data users must adhere to the policies and guidelines associated with the data they access.

3.14 **Encryption:** The process of converting data into a code to prevent unauthorized access. Encryption ensures that data remains confidential and secure while stored or transmitted over networks.

3.15 **Internal Data:** Data that is meant for internal use within the University and should not be disclosed to the public. While it does not contain personally identifiable or highly sensitive information, it may still require some level of protection to prevent misuse or inconvenience. Examples include internal communications, meeting minutes, and departmental schedules.

3.16 **Personally Identifiable Information (PII):** Any information that can be used to identify an individual, either directly or indirectly. This can include names, addresses, phone numbers, Social Security numbers, email addresses, and other personal data.

3.17 **Public Data:** Data that is freely available to the public without restriction. Public data does not contain sensitive or private information and poses no significant risk if exposed. Examples include general University information such as course catalogs, marketing materials, and press releases.

3.18 **Restricted Data:** Highly sensitive data that, if disclosed or misused, could cause severe harm to individuals or the University. Restricted data includes data governed by strict legal or contractual obligations, such as financial records, Social Security numbers, or proprietary research data.

3.19 **System of Record (SOR):** The authoritative data source for a given element or domain of information.

SECTION 4. POLICY

4.1. **Policy Statement**

4.1.1. Fairmont State University requires all institutional data to be entered in accordance with standardized formats, definitions, workflows, and validation rules. Data must be accurate, complete, timely, and compliant with all applicable regulations, including FERPA, HIPAA, Gramm-Leach-Bliley Act (GLBA), and institutional security policies. All departments must adopt or develop procedures consistent with this policy, and all users must follow these standards when entering or modifying institutional data.

4.2. **Accuracy**

4.2.1. Data must match authoritative documentation or verified sources.

4.2.1.1. Users must reference the institution-approved source documents (e.g., admissions records, HR forms, financial documentation, approved third-party data feeds). Each functional area defines its authoritative sources in its business processes maintained in a centralized digital repository with oversight by the Data Governance Committee.

4.2.2. Users must validate information before committing entries.

4.2.2.1. Validation includes cross-checking data against official documents, using system validation tools, and confirming unclear information with the appropriate data-owning department. Validation steps will be defined in system- or department-specific procedures.

4.2.3. Erroneous data must be corrected following approved correction procedures:

4.2.3.1. Each system of record (e.g., SIS, HRIS, Finance) maintains a documented Data Correction Procedure that outlines who may request or perform corrections, required documentation, approval steps, and timeframes. Corrections must be logged according to audit requirements (e.g., system audit trails, ticketing systems, or designated change logs). High-impact or sensitive data corrections require review by the data steward or data manager for that domain.

4.2.4. Data Stewards (determined by staff position) for each functional area, in coordination with IT system owners and the Data Governance Committee approves these procedures.

4.2.5. Only approved codes, values, and naming conventions may be used.

4.2.5.1. This is enforced through the following mechanisms: Systems of record must use controlled vocabularies, drop-down lists, and validation rules to restrict data entry to approved values. Data Stewards maintain the official lists of codes, values, and naming conventions. Changes to values or naming standards require the approval processes defined by the Data Governance Committee.

4.2.6. Required fields must be determined and maintained by designated data governance roles.

4.2.6.1. Data Stewards, in consultation with functional data owners and system administrators, identify the required fields for each system and process. Required fields are documented in system-specific data standards and configuration documentation. Any changes to required fields must follow the Data Governance Committee's change-management process.

4.3. **Completeness**

4.3.1. All required fields must be populated prior to submission.

4.3.2. Placeholder text (e.g., TBD, XXX, NA without cause) is prohibited unless explicitly permitted by the system owner.

4.3.3. Records must include all data elements necessary for downstream processes (e.g., payroll, billing, reporting).

4.3.3.1. All records should be formatted in a consistent manner.

4.4. **Timeliness**

4.4.1. Time-sensitive data (e.g., payroll deadlines, student enrollment updates) must follow the timelines set by the responsible department unless governed by an external entity. Delays must be documented if they impact compliance or operations.

4.5. **Security and Access**

4.5.1. Users may enter or modify data only within their approved security roles.

4.5.2. Sharing login credentials is strictly prohibited.

4.5.3. Systems must maintain audit trails of all data entry activity.

4.5.4. Sensitive data may only be handled according to Fairmont State's Protection of Confidential or Sensitive Information - Employee Agreement.

4.6. **Roles and Responsibilities**

4.6.1. Data Governance Committee / Data Governance Lead

4.6.1.1. Define and approve data standards, policies, and procedures. Ensure cross-departmental coordination and accountability for data quality. Monitor

compliance, risks, and performance metrics related to data governance. Review and approve changes to required fields, naming conventions, code sets, and correction procedures.

4.6.2. Operational Data Management Roles

4.6.2.1. Data Owner

4.6.2.1.1. Typically a senior leader responsible for a specific data domain (e.g., Registrar for student data, HR Director for employee data). Define access rights, data quality expectations, and authoritative sources for the domain. Approve major changes to data structures, required fields, or usage policies. Sponsor and oversee domain-specific data quality efforts.

4.6.2.2. Data Steward

4.6.2.2.1. Designated staff member(s) responsible for managing the accuracy, completeness, and consistency of data within their domain. Monitor data quality, perform routine validation, and coordinate error correction. Maintain lists of approved codes, values, and naming conventions. Collaborate with Data Owners, Information Technology (IT), and Institutional Research to enforce standards. Document domain-specific procedures for data entry, validation, and correction.

4.6.2.3. Data Custodian

4.6.2.3.1. Usually technical staff (often within IT) responsible for the systems that store and process data. Manage system configurations, backups, and overall data security. Implement and maintain access controls aligned with Data Owner approvals. Ensure that validation rules, required fields, and audit trails are technically enforced where feasible.

4.6.3. Institutional Units with Data Responsibilities

4.6.3.1. Data-Owning Departments (HR, Registrar, Finance, etc.)

4.6.3.1.1. Develop and maintain detailed, department-specific data entry and correction procedures aligned with this policy. Procedures should include dual review of data to the extent possible. Train staff on proper

data entry and validation methods. Monitor accuracy and correct errors promptly following approved procedures. Identify domain-specific authoritative documents and required fields.

4.6.3.2. Institutional Research (IR)

4.6.3.2.1. Provide operational data governance guidance and support. Conduct periodic data quality assessments and report findings to the Data Governance Committee. Publish institutional data definitions, code sets, and data dictionaries. Assist departments and Data Stewards in defining authoritative sources and required fields.

4.6.4. Technical Roles

4.6.4.1. Information Technology (IT) Services

4.6.4.1.1. Maintain system security roles, authentication, and access controls. Configure systems to enforce validation rules, formatting standards, and required fields where technically feasible. Oversee system audit logging and retention. Support Data Custodians and DBAs in maintaining reliable data systems.

4.6.4.2. Database Administrator (DBA)

4.6.4.2.1. Manage and optimize databases for performance, reliability, and security. Support legacy systems and implement enhancements or new database deployments. Maintain backups, recovery plans, and data integrity controls. Assist in implementing domain-specific validation, indexing, and structural rules that support data quality.

4.7. **Data Quality Assurance**

4.7.1. Data quality assurance is led by the Data Governance Committee, with Data Stewards responsible for operational monitoring, Data Owners accountable for domain-level performance, Institutional Research supporting measurement, and IT enforcing system-based controls.

4.7.2. The following quality measures will be assessed quarterly:

Criteria	Target	Description

Accuracy	≥ 98% correct entries	Sampled records match authoritative sources.
Completeness	100% required fields	No missing mandatory fields.
Consistency	95% adherence	Formatting and code standards followed across systems.
Timeliness	95% on-time	Entries completed within required deadlines.

4.8. **Review and Revision**

4.8.1. This policy will be reviewed every two years by IT and IR or as needed based on regulatory, technological, or operational changes.

SECTION 5. COMPLIANCE *(The policy's relationship to laws, regulations, and/or policies.)*

5.1. This policy is designed to ensure that the use, management, and protection of institutional data comply with relevant federal, state, and University-specific laws, regulations, and standards. The policy aligns with the following:

5.1.1. Federal Regulations

5.1.1.1. **Family Educational Rights and Privacy Act (FERPA)**: This policy ensures that all data handled in the ERP, particularly student data, is managed in accordance with FERPA requirements, safeguarding the privacy and confidentiality of student records.

5.1.1.2. **Health Insurance Portability and Accountability Act (HIPAA)**: In cases where the ERP stores or processes health-related data, this policy mandates compliance with HIPAA to protect the privacy and security of health information.

5.1.2. State Regulations

5.1.2.1. **West Virginia Data Breach Notification Act (WV Code § 46A-2-1501 et seq.):** This policy adheres to the West Virginia Data Breach Notification Act, which requires institutions to notify affected individuals in the event of a data breach involving personal information. Compliance with this law ensures that the ERP's data management systems are prepared to handle and report any breaches appropriately.

5.1.2.2. **West Virginia Privacy and Data Security Laws:** The policy ensures that ERP data practices align with state regulations surrounding data privacy and security, including any specific laws relating to the management of student, employment, or health-related information.

5.1.2.3. **West Virginia Freedom of Information Act (FOIA):** The ERP data is subject to disclosure under public records requests in accordance with the West Virginia Freedom of Information Act. This policy ensures that all data in the ERP is considered a public record is managed in accordance with the provisions of the FOIA.

5.1.3. University Policies

5.1.3.1. **Data Governance Policies:** This policy aligns with broader University Data Governance standards, which define how institutional data is classified, stored, and shared across systems.

5.1.3.2. **Data Security Policies:** All users of the ERP are required to comply with the University's data security policies to ensure that data is accessed and maintained in a secure manner, reducing the risk of unauthorized access or data breaches.

5.1.4. Consequences for Non-Compliance

5.1.4.1. Non-compliance with this policy may result in violations of federal, state, or institutional regulations, leading to corrective actions, including disciplinary measures, sanctions, or loss of access. Violations of this policy may also result in mandatory retraining and departmental findings during audit review.

SECTION 6. REVISION HISTORY *(A record of all changes made to the policy.)*

6.1. FREQUENCY OF REVIEW: This policy shall be reviewed at least every three (3) years, or more frequently as needed to reflect changes in legal requirements, institutional practices, or data governance standards.

6.2. APPROVED: Click or tap here to enter text

6.3. REVISED: Click or tap here to enter text