Administrative Policy #: 1303
Title: System of Record
Effective Date: Jan. 27, 2026

SECTION 1. PURPOSE & SCOPE

1.1. PURPOSE: The purpose of this policy is to establish an official system of record for student, academic, and related administrative University data. (The system of record is currently Banner.) By designating a single authoritative source, the University ensures consistency, accuracy, compliance, and appropriate stewardship of institutional data.

1.2. SCOPE: This policy applies to all University faculty, staff, administrators, and other authorized users who access, enter, update, or use data in the system of record or in any system that transmits data to or receives data from the system of record.

SECTION 2. APPROVAL, DELEGATION & APPLICABILITY

2.1. AUTHORITY: The Chief Information Officer has the authority to make decisions, enforce rules, and delegate authority related to this policy.

2.2. DELEGATION: Authority may be delegated to the Data Governance Steering Committee.

2.3. APPLICABILITY: This policy applies to: Individuals – All University faculty, staff, administrators, 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 system of record's self-service application are subject to applicable student use and data privacy policies but are not considered under the primary scope of this policy.

SECTION 3. DEFINITIONS

3.1. ANCILLARY SYSTEM: Any third-party application, database, or tool that uses, stores or derives data from Banner.

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

3.3. ENTERPRISE RESOURCE PLANNING (ERP): An ERP is a comprehensive, integrated software system that supports and connects key institutional functions—such as student information, enrollment, financial aid, finance, human resources, payroll, and advancement—within a single platform. By centralizing data and streamlining processes across academic and administrative units, an ERP helps institutions improve operational efficiency, enhance the student experience, support compliance and reporting, and enable data-informed decision-making.

3.4. PRINCIPLE OF LEAST PRIVILEGE / DATA MINIMIZATION: Users and systems are granted the minimum level of access and only the specific data necessary to perform their assigned responsibilities. Access rights do not exceed what is required for legitimate business, academic, or operational needs. Data collection, storage, and sharing must be limited to the smallest amount of information needed to fulfill an approved purpose, reducing risk and protecting institutional and personal data.

3.5. SYSTEM OF RECORD (SOR): The authoritative data source for a given element or domain of information.

SECTION 4. POLICY

4.1. DESIGNATION

4.1.1. Banner is designated as the University's system of record for student, academic, enrollment, financial aid, and other related administrative data. Oasis, is the state-managed payroll application, which is classified as an ancillary system used exclusively for payroll processing and disbursement. While Oasis processes payroll transactions, Banner remains the authoritative source for employee records. In cases of data discrepancies between Banner and Oasis, Banner shall prevail as the single source of truth for institutional records.

4.1.2. Data stored in Banner shall be regarded as the authoritative institutional source for reporting, compliance, and decision-making purposes.

4.2. DATA ENTRY AND MAINTENANCE

4.2.1. Authorized personnel are responsible for ensuring timely and accurate data entry into Banner, following established procedures.

4.2.2. Updates, corrections, and overrides to data must be performed directly in Banner to ensure data accuracy and integrity.

4.3. USE OF ANCILLARY SYSTEMS

4.3.1. Other systems may interface with Banner or temporarily store institutional data. However, Banner shall remain the authoritative data source.

4.3.2. In cases of discrepancies between Banner and ancillary systems, Banner shall prevail as the official record, unless a formal exception is approved by the Data Governance Committee.

4.3.3. Ancillary System integrations with Banner shall follow the principle of 'least privilege/data minimalization'. This means that only the minimal amount of access/data will be provided for the ancillary system to function. Ancillary systems that request Banner 'data dumps will require approval from the Data Governance Committee.

4.3.4. Ancillary Systems that require/request Personally Identifiable Information (PII) will require approval from the Data Governance Committee.

4.4. ACCESS AND SECURITY

4.4.1. Access to Banner is granted based on job function, role, and in compliance with relevant federal and state regulations, including FERPA and HIPAA where applicable.

4.4.2. All users must complete the required training and adhere to University data security policies.

4.5. GOVERNANCE AND OVERSIGHT

4.5.1. The University Data Governance Committee provides oversight for the designation and use of Banner as the system of record.

4.5.2. Regular audits and data quality reviews will be conducted to ensure compliance, accuracy, and integrity of data maintained in Banner.

4.6. EXCLUSIONS

4.6.1. Any exceptions to this policy must be formally requested and approved by the University Data Governance Committee.

4.6.2. Violations of this policy may result in loss of access to Banner, disciplinary action, or other corrective measures as outlined in University policies.

SECTION 5. COMPLIANCE

5.1. COMPLIANCE: This policy is designed to ensure that the use, management, and protection of institutional data stored in Banner 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 Banner, 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 Banner 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 Banner'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 Banner 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): Banner 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 Banner that is considered a public record is managed in accordance with the provisions of the FOIA.

5.1.3. Institutional Accreditation and Reporting Requirements: Banner serves as the authoritative source for institutional data required for reporting to accreditation bodies, governmental agencies, and other external stakeholders. This policy ensures that Banner is maintained to meet these requirements and that data integrity is preserved for official reporting.

5.1.4. Compliance Audits and Reviews: The University Data Governance Committee will conduct periodic audits and reviews of data within Banner to assess compliance with this policy and relevant external regulations.

5.2. NONCOMPLIANCE: Failure to comply with this policy may result in corrective actions, including remediation, restricting or revoking access, training, or disciplinary measures.

SECTION 6. REVISION HISTORY

6.1. FREQUENCY OF REVIEW: This policy will be reviewed every year or upon significant changes to technology, security practices, or University priorities.

6.2. APPROVED: Approved by the President on January 27, 2026.