FINAL POLICY

Policy Name	Administrative Data Management and Access Policy
Policy Category	Digital Strategy and Infrastructure
Policy Sub-Category	Information and Security
Policy Approved By	Cabinet
Responsible VP	Vice President for Digital Strategy and Infrastructure & CIO
Responsible Department	Digital Strategy and Infrastructure
Responsible AVP or Director	Deputy CIO
Original Policy Date	1/24/2012
Last Known Revision Date	1/24/2012
Date of Policy Review	1/24/2012
Policy Effective Date	1/24/2012
Recommended Policy Review Date	3/2/2019
Policy Applies To	All Employees
Additional Authority/References	Click or tap here to enter text.

Policy Purpose

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain data quality or integrity.

The purpose of this policy is to define access, controls, and protection of the college's administrative data. Administrative data maintained by the institution is a vital information asset that will be available to all employees who have a legitimate need for it, consistent with the institution's responsibility to preserve and protect the integrity of the data and to ensure the privacy of sensitive data.

The institution is the owner of all administrative data; individual units or departments have stewardship responsibilities for data domains or portions of the data.

Designated Albright College data domains, data trustees, and data stewards are listed in Appendix A – (Listing of Albright College Data Trustees and Data Stewards) of this policy. Adjustments to Appendix A will be incorporated as necessary over time, as additional enterprise data management systems are implemented, or as organizational and staffing changes warrant. Such changes will not be deemed a revision to this policy.

Applicability

Administrative data captured and maintained at Albright College are a valuable college resource. While these data may reside in different database management systems and on different machines, these data in aggregate may be thought of as forming one overarching, enterprise administrative database.

This policy applies to all users of Albright's administrative database environment.

Policy

Access to non-public administrative data is granted only via the appropriately designated Albright College Data Steward.

By authorizing access to designated categories of administrative data, Data Stewards are acknowledging a legitimate user need for information access, as well as appropriate training and understanding on the part of the requesting user to ensure ongoing administrative data integrity, quality, protection, and privacy. In addition to authorizing new administrative data access requests, Data Stewards are responsible for an annual review of user security access to their respective data domains.

By receiving access to designated categories of administrative data, the requesting data user is acknowledging responsibility for adherence to all relevant Albright policies, procedures, standards and guidelines.

The college has defined three levels of data classification for administrative data:

- Public Data
- Restricted Data
- Highly Sensitive Data

Additional safeguards and protocols exist to further protect both Restricted and Highly Sensitive data, as appropriate.

Data Classifications

Public Data – General administrative data that are intentionally made public are classified as Public Data. This includes all general administrative data that are not legally restricted or judged by Data Stewards to be limited access data. Examples of Public Data include the Albright Master Course Schedule as well as faculty, staff and student directory data. Public Data are often readily available on Albright's public website.

Restricted Data – By default, all administrative data not explicitly defined as either Highly Sensitive or Public are classified as Restricted Data. Examples of Restricted Data include student grades and faculty/staff salaries.

Appropriate safeguards, including data access authorization and approvals by Data Stewards, must exist for all data that the college is obligated to protect, whether by law, contract, or college policy. Secure credentials are required to access restricted university data. Standards or guidelines governing the access, release, distribution and dissemination of restricted data by individuals authorized to access it is controlled and administered by the designated Data Stewards.

Highly Sensitive Data – Highly Sensitive Data are by definition restricted and include personal information that can lead to identity theft if exposed or disclosed in an unauthorized manner. Specifically, the college defines the following as Highly Sensitive Data:

The first name or first initial and last name in combination with and linked to any one or more of the following data elements about the individual:

- Social security number
- Driver's license number or state identification card number issued in lieu of a driver's license number
- Passport number; or
- Financial/banking account number, credit card number, or debit card number.

Electronic Storage of Highly Sensitive Data Procedures – Additional safeguards and protocols exist to ensure Albright constituent privacy and to protect Highly Sensitive Data from unauthorized exposure. Like Restricted Data, access to Highly Sensitive Data may only be authorized by Data Stewards. Further, Highly Sensitive Data must not be stored or kept on any

non-network storage device or media. Prohibited storage media includes storage on desktop computers, laptop computers, PDAs, cell phones, USB drives, thumb drives, memory cards, CDs, DVDs, local external hard drives and other USB devices unless specifically approved encryption methodologies have been utilized.

Further, Highly Sensitive data cannot be distributed, including via e-mail or e-mail attachment, unless via approved encrypted means.

Exceptions to the procedures for the electronic storage of Highly Sensitive Data must be approved by the appropriate division Vice President in consultation with the Chief Information Officer. Approved exception requests will be documented to ensure the implementation of acceptable data encryption protocols.

RESPONSIBILITY OF DATA TRUSTEES, DATA STEWARDS AND DATA USERS

Data Trustee: Data Trustees are the senior College officials (typically at the level of Vice President) who have planning and policy-level responsibilities for data within their functional areas and management responsibility for defined segments of institutional data, or data domains. The Data Trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability. Data Trustees typically serve as the executive sponsors of technology projects involving institutional data management.

Data Trustees work with the Chief Information Officer to prioritize data management related projects and to ensure that the appropriate resources are available to support the data needs of the College.

Data Trustee responsibilities include:

- Assigning and overseeing Data Stewards
- Overseeing the establishment of data policies in their areas
- Determining legal and regulatory requirements for data in their areas
- Promoting and ensuring appropriate data use and data quality
- Addressing institutional data issues that a.) potentially compromise data integrity, reliability, privacy or b.) potentially limit or reduce institutional effectiveness or efficiency

Data Stewards: Data Stewards are appointed by Data Trustees. Data Stewards have primary responsibility for the accuracy, integrity, privacy, and security of the College Data under his/her

stewardship. They have overall responsibility for appropriate system use and data maintenance procedures within their areas, including the administration of any additional policies or procedures to govern the use of legally protected, restricted or sensitive college data. Additional responsibilities include:

- Communicating with and educating data users on appropriate use and protection of institutional data
- Developing and documenting procedures for requesting and authorizing access to restricted administrative data.
- Testing, approving, and authorizing the production implementation (or 'go-live') of new, upgraded, or updated software programs pertaining to administrative data management and software systems (such as PowerCampus, PowerFaids, Great Plains, and Millenium, etc.).
- Working with Information Technology Services and appropriate Records Management officials to determine data retention requirements and archiving strategies for storing and preserving historical operational data.
- Working with ITS and the Data Management Group to ensure that a common set of data definitions is consistently used and applied, to facilitate data-driven decision making, to enhance the ability for automated system interfaces, and to generally improve the electronic exchange of data across the enterprise.
- Assure data integrity, respond to questions about the accuracy of data, and correct inconsistencies.
- Assure data collection is complete, accurate, valid, timely, and that data are maintained as close as is possible to the source or creation point of the data.
- Establish and maintain business rules regarding the manipulation, modification, or reporting of administrative data elements and for creating derived elements in support of accurate data integration efforts, automated business process improvement projects, or other college planning and assessment efforts.
- Work with Information Technology Services to monitor and periodically review (at least once annually) individual user security profiles and authorized data access.

Data Users: Data Users are the individuals who access college data (in accordance with authorization by the appropriate Data Steward) in order to perform their assigned duties or to fulfill their role in the college community. Data Users are responsible for protecting their access and authentication privileges, the proper use of the college administrative data and the protection of confidentiality and privacy of individuals whose records they access. Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted the ability to view, copy, download, create, modify or delete.

Data Management Group: A college-wide group composed of Information Technology Services management, Data Stewards, and interested Data Users which meets regularly to review data management activities and planned projects and upgrades, as well as to generally communicate and coordinate regarding relevant business rules, data integration, systems interoperability, and business process improvement. The Data Management Group makes recommendations to Data Trustees, as appropriate. It is the responsibility of Information Technology Services to convene and coordinate Data Management Group meetings.

Decision

☒Approved President's Advisory Council

☐Rejected_____

☐Tabled or Further Review Needed_____

Comments:

Policy Maintained By

Digital Strategy and Infrastructure

Revision Log

Approved by President's Advisory Council, January 24, 2012

APPENDIX A (Listing of Albright College Data Trustees and Data Stewards)

Data Domain	Data Trustee	Data Steward
Traditional Undergraduate Admission Data	VP for Enrollment Management	Director of Enrollment & Information Services
SPS Admission and Student Data	Provost and SVP for Academic Affairs	Dean, School of Professional Studies
Graduate Admission Data	Provost and SVP for Academic Affairs	Dean, School of Professional Studies
Traditional Student Academic Data, Course Schedules and Enrollment Data	Provost and SVP for Academic Affairs	Registrar
Housing Data	SVP for Student and Campus Life and Chief Health Officer	Director of Housing & Residential Learning
Student and Campus Life / International Students & Community Standards	SVP for Student and Campus Life and Chief Health Officer	Dean of Students
Health Services Data	SVP for Student and Campus Life and Chief Health Officer	College Physician
Finance & Student Accounting Data	VP for Finance & Strategic Partnerships	Associate VP for Administrative and Financial Services / Controller
ID Card/Access Data ID Card/Dining, Vending, Debit	SVP for Student and Campus Life and Chief Health Officer VP for Finance & Strategic Partnerships	Director of Public Safety and Associate VP for Administrative and Financial Services / Controller
Human Resource Data	SVP Student and Campus Life and Chief Health Officer	Director of Human Resources
Payroll Data	VP for Finance & Strategic Partnerships	Associate VP for Administrative and Financial Services / Controller
Public Safety Data	SVP for Student and Campus Life and Chief Health Officer	Director of Public Safety
Student Financial Aid Data	VP for Enrollment Management	Director of Financial Aid
Advancement /Alumni Data	VP for Advancement	Gift Processing Coordinator

Athletics Data	Co-Directors of Athletics	Head Swim Coach/Director of Aquatics
Learning Management System	Provost and SVP for Academic Affairs	Learning Management System Administrator
Parent Data	VP for Advancement	Gift Processing Coordinator
Comparative Institutional Data	Provost and SVP for Academic Affairs	Director, Institutional Research
Student Success Data	Provost and SVP for Academic Affairs	Student Success System Administrator