Policy Number	708 000
Policy Title	Data Governance Policy
Responsible Officer	Vice President of Information Technology
Responsible Office	Information Technology
Summary	The purpose of data governance is to establish a culture that ensures that CIU institutional data is both secure and available to those who should have access to it. This policy establishes guidelines for governing data access, report access, and email distribution list access.
Definitions	Data-Any electronic information stored in databases, applications, emails, and/or reports and is sometimes referred to as an electronic record, file, letter, email, or account.
Approving Body	12.08.2023 (Acad C); 11.15.2023 (Admin C)
Approval Date	12.08.2023
Re-evaluation Date	Fall 2026
Departmental Impact	All departmental users who access data, reports, and email distribution records from CIU databases.

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy Statement

This policy serves as guidance to CIU data owners, managers, and users, including BLS users who access and use data from CIU applications. Data is a vital institutional asset that must be used legally and ethically. Requests for data are subject to many considerations, including:

- Data sensitivity
- Compelling institutional need
- Reputational risk
- Confidentiality
- Privacy
- Support staff resource availability

Rationale

CIU information and records are vital for essential business workflows of the organization. Some data, as containers of records, are historical or are legally required to be maintained for certain time periods. Data that fits either of these requirements must be preserved or disposed of in accordance with the organization's records retention policy and retention schedule.

The scope of this policy encompasses data, records, and information entered, maintained, and exported from enterprise software applications and databases such as enrollment management systems, financial aid systems, student information systems, personnel management systems, accounting systems, customer relationship management systems, file management systems, inventory systems, learning management systems, email systems, and document management systems. This policy does not pertain to intellectual property, social media, or web content data.

Roles Required to Govern CIU Data

Several groups govern the management of, access to, and accountability for CIU data.

Administrative Council - This council is comprised of department administrators from across all functions and departments of the organization. This group adds shared accountability and collaboration to approve policies that impact the governance of institutional data.

IT Advisory Council - This council is comprised of department representatives providing steering advice to the VP of Information Technology regarding all technical matters of the organization, which includes data governance. This group adds shared accountability and calibration to recommend policies to the Administrative Council to protect all IT assets, including data assets and systems that house data.

Data Stewardship Subcommittee – The Data Stewardship Subcommittee is a focus group of the IT Advisory Council comprised of representatives responsible for identifying and establishing guidelines for data owners, identifying improvements with data usage and protection, and recommending standard practices and tools used for handling data. The Data Stewardship Subcommittee recognizes the importance of and raises awareness of sound data management across the organization. This group adds shared accountability and collaboration to our practices to provide clear and consistent responses to data requests. The Data Stewardship Subcommittee, with Data Owners, annually (minimum) reviews each user's access to institutional data and determines if there is questionable access granted.

Data Owners – Data Owners are senior institution officials who have planning, policy-level and management responsibility for data within their functional areas. (Refer to Data Owner Assignments)

Data Managers – Data Managers are individuals who are responsible for data collection, quality control, processing, and management for their functional area.

Data Users – Data Users are college units or individual faculty or staff who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the organization; this access is granted solely for the conduct of institutional business. Data users include Ben Lippen employees who access and use data from CIU applications.

IT Support Staff – Database Administrators and other IT staff who are responsible for maintaining technical systems that house and protect data.

Policy Procedures

Responsible stewardship of university data is critical to the work of the college and required in order to ensure those with official educational or administrative responsibilities can access and rely on the accuracy and integrity of the data. Data managers are expected to comply with the following data policies and manage data within their care in a manner that is consistent with legal, ethical, and practical considerations.

Data Access

Data access is granted to those with legitimate educational or business interest in the data. Access is granted by IT or the appropriate Data Manager and may require approval of a Data Owner. See Figure A for a flowchart representing the process.

Improper release, maintenance or disposal of institutional data may be damaging to the organization and expose CIU to significant risk and possible legal action. Those granted access to college data must agree to the following guidelines.

1. Maintenance of data must strictly adhere to the policies and procedures of CIU. Unauthorized use, disclosure, alteration, or destruction of data is prohibited.

2. Data Owners, as defined in the roles policy, may grant access to data if it needs to be shared with others. Others seeking data access, including Data Managers and users, must seek approval from the relevant Data Owner before using that data.
3. Data may not be released to third parties or others at the college who do not have access to the data without the consent of the appropriate Data Manager and must always be done in compliance with all laws and regulations (e.g., FERPA, HIPAA, and GDPR).
4. The institutional need must be demonstrated in order for access to be granted by the Data Owner.
5. If the Data Owner is uncertain about releasing data, the decision should be elevated to the IT Advisory Council by the Data Stewardship Subcommittee. In the event the IT Advisory Council is unable to make a decision, the VP of Information Technology will escalate the discussion to the Administrative Council.
6. Access to and use of data is restricted to the scope of an individual's work. Data should not be viewed or analyzed for purposes outside of official business.
7. Access is granted for specific purposes and durations, the data may not be used for other purposes or kept beyond its need.
8. All data must be used, transmitted, and stored according to departmental policies and procedures adhering to applicable state and federal regulations or industry best standards.
9. Any actual or suspected loss, theft, or misuse of data must be reported to the Data Owner, the Data Manager, and OIT immediately.

All security and computer use policies must be adhered to, which are primarily articulated in the IT Acceptable Use Policy and Security Management Policy.

Data Audits

Periodic data audits will be performed by the Office of Information Technology to review data access with the appropriate Data Owners. The Office of Information Technology will develop procedures and an audit schedule to effectively perform audits throughout the academic year.

Classification of Data

Accurate classification provides the basis to apply an appropriate level of security to college data. All data within the organization are classified into four levels of sensitivity to provide a basis for understanding and managing data. These classifications take into account the legal protections (by statute, regulation, or by the data subject's choice), contractual agreements, ethical considerations, or strategic or proprietary value. They also consider the application of "prudent stewardship," where there is reason to protect the data to protect individuals or the organization.

The classification level assigned to data guides Data Owners, Data Managers, and Data Users in the security protections and access authorization mechanisms appropriate for those data. Such categorization encourages discussion and subsequent full understanding of the nature of the data being displayed or manipulated.

Classification Levels

Data classifications are usually determined by Data Owners, Chief Information Officer and/or federal laws. There are four levels of classification for our data (refer to Rationale and Definitions sections). They are listed below.

Public Data – low level of sensitivity
Internal Data – moderate level of sensitivity
Confidential Data – confidential information
Protected Data – highest level of sensitivity

Report and Email Distribution List Access

Like data, access to reports generated by CIU enterprise applications and email distribution groups are granted to those with legitimate educational or business interest. Access is granted by the Office of Information Technology or the

appropriate Data Manager and may require the approval of a Data Owner. To request access to a report or email distribution group, submit an IT ticket.

Data Owners, Managers, and Access Vetting Process

A list of data owners, managers, and the process to evaluate data, report, and email distribution access requests is established by the Data Stewardship Subcommittee. The listing can be found here.

Hyperlinks

www.ciu.edu/policy

Revision Table