CSU Data Governance Plan

Columbus State University's (CSU) Data Governance Plan was developed to comply with the University System of Georgia's (USG) Business Process Manual Section 12. Data Governance and Management. The document provides guidance on Governance Structure, Data Management, Cybersecurity, Compliance, and Data Privacy.

The Data Governance Committee is responsible for defining, implementing, and managing policies and procedures for data governance and data management across CSU campus.

Responsibilities include but are not limited to the following:

- Defining data management roles and responsibilities
- Maintaining documentation related to data governance and management policy and procedures in a centralized location.
- Identifying the Data Governance and Management Committee structure and membership
- Ensuring that cybersecurity and data privacy control processes are operational
- Defining communications to instill data privacy values, and
- Assisting the chairs of the functional and technical committees to ensure effectiveness.

Levels of Data Governance Responsibility

The levels of responsibility for data management are:

Data Owner
The President of the institution is identified as the Data Owner. The Data Owner has the ultimate responsibility for submission of organizational data to the USG and the accountability of Data Trustees. The role of the Data Owner is to ensure that an appropriate data governance structure is in place, operating effectively, and supported by other institutional leaders.

Data Trustees
Data trustees are the executives of the organization and have overall responsibility for the data processed in their data areas. These individuals are usually cabinet-level positions reporting directly to the President. The Data Trustees appoint data stewards within each functional area for which they are responsible, and communicate unresolved concerns about data quality, security, privacy and compliance.

Data Stewards
Data Stewards are the individual identified by the Data Trustees to be responsible for the data processed and the technology used to do so in their data areas. The Data Stewards recommend policies and establish procedures and guidelines concerning the accuracy, privacy, and integrity of the data for which they are responsible; develop standard definitions for data elements created and/or used within the functional unit; ensure data quality standards are in place and met; and communicate concerns about data quality, security, privacy and compliance to the Data Trustees.

Data Users
Data Users are any faculty or staff who have access to university data as part of assigned duties. This role includes staff members who have direct responsibility for entering and using data. Daya Users will use data as intended and in compliance with applicable regulations; follow security policies and procedures and report violations or problems to the Chief Information Security Officer; and report issues with data quality, availability or misuse to the Data Stewards.

Chief Information Officer (CIO)/Chief Information Security Officer (CISO)
The responsibilities of the CIO and CISO are to ensure that technical infrastructure is in place to support the data needs and assets, including availability, delivery, access, and security across their operational scope.

View the members of the CSU Data Governance Team

Data Management
CSU ensures that data is being managed effectively by following data system documentation, data elements and definitions, data quality, and data availability.

Data System Documentation
CSU maintains a listing of mission-critical data systems along with information essential to the effective loading, maintenance, use of, as well as reporting from, those systems.

Data Elements & Definitions
For systems that are part of routine data collection and reporting, data element dictionaries are maintained.

Data Quality
CSU ensure that information is of the highest possible quality to facilitate effective decision-making.

Data Availability
For all data domains and their respective data systems, CSU documents and socializes to data users the expectations and processes around the availability of each data resource.

Data Lifecycle
CSU ensures the data retention and destruction policies and procedures comply with the USG policy referenced at USG Records Management

Cybersecurity
Cybersecurity refers to preventative methods used to protect information and information systems, products and services from unauthorized access, compromise or attack. Cybersecurity requires an understanding of potential threats and utilizes strategies that include, for example, identity management, risk management and incident management.

Safeguards
CSU ensures that cybersecurity safeguards are established, in place, effective and adhered to in order to reduce risk. This applies to all users of USG information resources. Safeguards include policies, procedures, requirements, and practices that are necessary for maintaining a secure environment for the storage and dissemination of information. The benefits of safeguards include identification of fraud, security vulnerabilities, unforeseen threats and minimization of potential impacts.

Classification
CSU employs a classification structure for each record to ensure appropriate protection from unauthorized use, access, disclosure, modification, loss or deletion, The classification tier includes Unrestricted/Public Information, Sensitive Information, Confidential Information. In addition, Personal Information may occur in unrestricted/public, sensitive, and/or confidential information. It is information that identifies or describes an individual and must be considered in the classification structure

Access Procedures
CSU has a data trustee and data steward for each critical system or systems containing confidential or sensitive information and maintains a current list of users granted access to information systems. Only authorized users are allowed physical, electronic or other access to information systems. Data trustees, data stewards and users share the responsibility of preventing unauthorized access to the organizations' information systems. Data stewards will analyze user roles and determine the level of access required to perform a job function. The level of authorized access is based on Principle of Least Privilege. HR and/or the supervisor will notify the data steward of personnel status changes in job function, status, transfers, referral privileges or affiliation.

Segregation and Separation of Duties

In addition to having a well-organized and defined data governance structure, CSU ensures that its organizational structure, job duties, and business processes include an adequate system of separation of duties. Duties are divided among different individuals to reduce the risk of error or inappropriate action to accomplish separation of duties

Compliance
Through active measures CSU ensures compliance with external regulations through regular training, monitoring, and auditing as well as through policies and procedures developed through appropriate governance and administrative processes within CSU.

Each USG organization must have policies and procedures to ensure that appropriate organizational personnel have a working knowledge of:

FERPA
The Family Educational Rights and Privacy Act is a federal law that requires colleges and universities to protect the confidentiality of student education records.

HIPAAT
The Health Insurance Portability and Accountability Act is a set of federal rules designed in part to protect the privacy of a person's health information.

Georgia Open Records Act
The Georgia Open Records Act OCGA § 50-18-70 outlines the process for how members of the public can request and inspect government records.

GDPR
The General Data Protection Regulation is EU law on the protection of natural persons with regard to processing of personal data and on the free movement of such data.

Data Privacy
CSU is committed to protecting privacy. Personal information will only be disclosed to third parties when allowed by law or with the consent of the data subject.