ATHENS STATE UNIVERSITY

Policy Number: VI.06
Policy Level: Operating Policy
Originally Issued: April 1, 2022
Revised: July 14, 2023
Policy Owner: President
Policy Implementation: Chief Information Officer
and Information Security Officer

Data Governance

I. Policy Statement and Purpose

The confidentiality, integrity, access, and security of data is required whether it is physically stored on paper or digitally stored online. This policy applies to all University data and records whether the data is stored on a University owned or managed system or on a third party hosted service. Intellectual property is excluded from the scope of this policy.

Data management and data governance are managed collaboratively by the President and the Data Governance Council (DGC).

II. Definitions

Data Trustees - Data trustees will have high-level, administrative oversight and responsibility for institutional data systems and data sets managed by personnel reporting to them. The data trustees are responsible for the appointment, oversight, and accountability of data stewards.

Trustees oversee business practices in their areas of responsibility in respect to the quality, integrity, and integration of data systems; are responsible for following University established data access and security policies and procedures; and are charged with compliance oversight with federal and state laws.

Institutional Data Systems & Data Sets	**Data Trustee**
Student Recruitment CRM Data Set	Provost/VP for Academic Affairs
Student Information System Records	Provost/VP for Academic Affairs
Financial Aid Records	Provost/VP for Academic Affairs
Student Success records	Provost/VP for Academic Affairs
Financial Records	VP, Financial Affairs
Personnel Resources	VP, Financial Affairs
Common Aggregated Data Sets	VP, Academic Affairs
Assessment Data Sets	VP, Academic Affairs
Learning Management System Records	VP, Academic Affairs

Alumni Data Set	VP, University Advancement
Foundation Data Set	VP, University Advancement
Web Site	VP, University Advancement
Help Desk CRM Data Set	Chief Information Officer
University Portal Data Set	Chief Information Officer
Event Management/Work Order Data Set	Chief Information Officer
All Institutional Data & Metadata Repositories	Chief Information Officer

Data Stewards -Data stewards have high-level responsibilities for managing datasets with oversight from data trustees in functional areas. Data stewards are responsible for complete, accurate, valid, and timely data collection and providing accessible, meaningful, and timely machine readable institutional data for University use. Data stewards and the technology officials who manage systems share the responsibility for data compatibility, accessibility, and interfaces among institutional data elements. Data stewards and these technology officials will work together toward unification of the various data element coding structures and data storage formats which exist in various systems where institutional data are stored. Further delegation and decentralization of data collection and maintenance responsibility is encouraged in order to assure that 1) electronic data are collected and maintained as close as possible to the source or creation point of the data as identified by the data steward and 2) each manual or computer process which handles data adds value to the data.

Data stewards supervise and advise data managers and data users in the daily capture and processing of data. The data steward works closely with data and systems for processing and maintaining the data by following established University data access and security policies and procedures. Data stewards will also be responsible for meta data documentation and management including identifying and defining data used in internal and external reporting, the common data set content, the data dictionary, data sources, content, codes, business rules, data relationships, history of changes/modifications, and ERP upgrades/modifications that may impact data.

The data stewards are:

- Director of Admissions
- Assistant Director of Admissions for Recruiting
- Director of Student Success
- Student Success Lead Coach
- Director, Financial Aid
- Registrar
- Assistant VP Financial Affairs/Business Manager
- Assistant Provost for Planning, Budget and Assessment
- Director, Prospect Management
- Donor Relations Officer
- Client Systems Support Manager

Data Governance Council (DGC) – The Provost delegates the direct responsibility for data integrity to the Data Governance Council. The Data Governance Council is comprised of all data stewards along with an appointed ITS representative from the MIS area. The Data Governance Council will be responsible for establishing, monitoring, and reviewing institutional data governance policies and procedures to ensure protection of data quality, integrity, and integration consistently in the functional areas across the University. Additional responsibilities of the Data Governance Council include, but are not limited to:

- Establishing, reviewing, and monitoring the operational University databases used with all functional area information systems including the student information system, human resources information system, financial management system, advancement information system, and alumni information system.
- Reviewing and approving the metadata structure, data dictionary mappings, and use of the University databases associated with the systems listed previously and other databases used in the functional areas.
- Identifying and defining the roles and responsibilities of data stewards and data managers associated with each of the databases used at the University.

- Reviewing and approving the implementation, creation, modification, or deletion of key data elements and coding structures used in the University databases.

Data Integrity problems and issues should be reported to the Data Governance Council if needed to assist with cross-functional areas impacts on data integrity. Ultimately, the responsibility to resolve the data integrity issues lie with data managers, stewards, and trustees in functional areas where the data is entered, calculated, or reported.

Data Views may be defined in order to aggregate data from multiple sources into smaller and more manageable subsets, segregate data according to confidentiality or restriction characteristics that allow the resulting subset to be made available more widely for analysis or business processes. The data stewards are responsible for defining standard views of institutional data.

Data managers or data users may recommend the definition of new data views.

System Administration - Institutional data must be maintained within a single, logically-integrated information system. Institutional data may be stored on diverse computing hardware platforms that can be logically accessed and integrated to form an overall university information system.

If institutional data are stored on any component of the university information system, that system component must have defined a formal system administration function and have assigned to it a system administrator whose responsibilities include: physical site security; administration of security and authorization systems; backup, recovery, and system restart procedures; data archiving; capacity planning and performance monitoring.

University servers that are used to store limited-access data must comply with specific management standards. Web and other servers that must be accessible from off-campus must be physically separated from servers hosting limited-access institutional data. Direct access to university file servers hosting limited-access institutional data must be limited to on-campus authorized accounts. Individuals requiring direct access to files stored on these servers from off-campus must use the virtual private network (VPN) service.

User support - Data stewards will provide user support primarily through documentation of the functional information system resource and as needed to assist data users in the interpretation and use of institutional data. This responsibility may be delegated to the data managers.

III. Data Classifications and Access

Data stewards are responsible for setting policies regarding the manipulation, modification, or reporting of institutional data elements and for creating derived data elements.

Data stewards are ultimate responsibility for proper use of institutional data; individual data users will be informed of the rules governing the use and sharing of data.

All data extracted or reported from institutional data must include a record or display of the time and date of data capture.

Data stewards will work together to define useful and meaningful schedules for standard data extracts and the dates on which these will occur. These standard extracts of the data ("data snapshots") will also be considered institutional data.

As part of the data definition process, data stewards will assign each data element and each data view of institutional data to one of the following three classifications:

Confidential Data:
Data that is business or personal information that is required to be strictly protected. There are often governing statutes, regulations or standards with specific provisions that dictate how this type of data must be protected. Access to confidential data is limited to persons with authority to view or use the data and may not be shared with or disclosed to persons without such authority; it may be used only for those purposes that are a part of the employee's responsibility. Unauthorized disclosure of this information could have a serious adverse impact on the University, individuals or affiliates.

Regulations, laws, and standards that affect data in this category include, but are not limited to, the Health Insurance Portability & Accountability (HIPAA) and Payment Card Industry (PCI) standards, Family Education Rights & Privacy Act (FERPA) and the Graham-Leach-Bliley Act (GLBA).

Examples:
Biometric data, credit card information, passport numbers, state issued driver/non-driver license numbers, military identification, bank account number, health insurance policy number or subscriber information number, medical history, Social Security numbers, student data that is not designated directory information, certain research (e.g. proprietary or otherwise protected).

Operational data:
This data includes information that is not openly shared with the general public but is not specifically required to be protected by statue, regulation or by department, divisions or University policy. It is intended for the use by a designated workgroup, department or group of individuals with the University. Unauthorized disclosure of this information could adversely affect the University, individuals or affiliates.

While some forms of sensitive data can be made available to the public, it is not freely disseminated without appropriate authorization.

Examples:
Personally-identifiable-information (PII) such as name, birthdate, address, employee/student ID, etc. when held in combination in a way that could lead to identify theft or other misuses; budget information; personal phone numbers; employment applicant information; departmental policies and procedures; internal emails, documents or memos; incomplete or unpublished research; human resource information.

Public Data:
Data that is purposefully made available to the public by some valid authority and may be freely disseminated without potential harm to the University or its affiliates. Public data may be derived from operational data and contextually presented in aggregate for public viewing based on agreed upon report formats.

Examples:
Fact Book, Student Achievement Report; federal and state reporting; advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases, instructions, training manuals.

IV. Data Documentation

Documentation of data elements is the data steward's responsibility. However, some or all of these responsibilities may be assigned to data managers. The documentation of data is an iterative process. The documentation of data elements that are used most often for critical operational processes are considered to be the highest priority in the documentation process. Additionally, data elements that are used for analysis and reporting should be documented carefully in order to ensure the integrity of the data.

A data dictionary will be used record data definition characteristics and actively used to record any required modifications to the data elements. Changes to the data dictionary must be reviewed by the Data Governance Council in advance of the change. The University data dictionary can be viewed by any data trustee, steward, data manager, or requestor of data.

The following are considered to be important and valuable information to document about data elements.

Documentation/definition for data elements should include the following:

- Name and alias names
- Description of the data element
- Assigned data steward
- Usage and relationships to other data elements
- Update frequency
- Source for data capture
- Official data storage location and format
- Designation as "confidential”, "operational", or "public"
- "Confidential" data elements require a description or specification of the restriction
- Description of validation criteria and/or edit checks
- Description, meaning, and location of allowable codes
- Access rules and security requirements
- Archiving requirements
- Data storage location of extracts

Other vital data element documentation includes:

- Documentation for derived institutional data must include the algorithms or decision rules for the derivation.
- Documentation of data views must include reference to the data elements which comprise the view and description of the rules by which the view is constructed.
- Overview documentation for databases, files, and groups of files that include institutional data must also be provided, and must include information about data structure and update-cycles necessary for the accurate interpretation of the data.

V. Data Integrity, Validation and Correction

The data steward or delegated data manager is responsible for data integrity, responding to questions about the accuracy of data, and correcting inconsistencies if necessary.

Applications that capture and update institutional data must incorporate edit and validation checks to assure the accuracy and integrity (consistency) of the data. The accuracy of any element can be questioned by any authorized data user. The data user has the responsibility to help correct the problem by supplying as much detailed information as available, sufficient to permit understanding and diagnosis of the problem.

Upon written identification and notification of erroneous data, corrective measures must be taken as soon as possible to:

- Correct the cause of the erroneous data.
- Correct the data in the official storage location.
- Notify users who have received or accessed erroneous data.

VI. Data Security

University information and cyber security policies establish requirements and guidelines that are generally applicable to data security. The data steward will be responsible for interpreting and applying these security requirements to the management of data sets. Data stewards will responsible for assessing the specific security requirements applicable to the data sets under their management and establish the necessary access restrictions to ensure the security of the data.

All employees having access to any limited-access or systems that manage any institutional data will complete the Athens State University Data/System Access Form that formally documents the access to specific systems/modules/data sets/data views and conveys to the employee an understanding of the level of access provided and their responsibility to maintain the confidentiality of the data they access. The data steward and/or business process owner is responsible for monitoring and reviewing security implementation and authorized access.

The data steward is ultimately responsible for defining backup requirements for data sets and collaboratively developing with Information Technology Services the policies and procedures required to assure that data are backed up and recoverable in response to events that cause the loss or compromise of data whether accidental or intentional.

Information Technology Services will work closely with data stewards to develop the backup and recovery processes in accordance with the Incident Response/Recovery and Data Backup policy and will fully support the data steward and trustees' record retention and recoverability requirements as mandated by the state.

Unattended workstations that access confidential data should be secured and the screens not visible to individuals without access rights to the confidential data.

Individuals requiring access to central sources of confidential or operational data must be authorized by the appropriate data steward or manager by completing the requirements outlined on the Athens State University Data/System Access Form.

All systems and limited access data may be accessed through VPN access is approved by the appropriate Data Trustee.

Insecure protocols for connecting to all university systems, and for transferring data to and from those systems is prohibited, especially those servers that support critical operations and/or host limited-access data.

VII. Data Storage

The data steward is responsible for identifying an official data storage location for each data element, as well as an official data storage location of valid codes and values for each data element. The data steward will also determine archiving requirements and strategies for storing and preserving historical data for each data element.

Data element names, formats, and codes must be consistent across all applications which use the data and consistent with such university standards as are developed.

The Chief Information Officer and Director of Information Technology Services will assist by working with each functional area to determine data storage location and archiving requirements for institutional data.

Limited-access data must never be stored on individual user workstations, laptops, tablets, or any other type of electronic equipment. Limited-access data must be stored on registered, and properly configured and managed, department or central file servers.

Departments are expected to identify, for their users, appropriate server locations for storage of data extracted from central sources or derived through department operations. In addition, Information

Technology Services and the Information Security Officer will define the required restrictions for how data is stored and shared to protect data.

When limited-access university data are stored on appropriate servers, they must not include SSNs unless they are keys to linking with other files. SSNs must not be collected from individuals nor extracted from central systems and stored on departmental servers unless doing so is absolutely required to maintain the business functions of the office involved.

So that standards for survey research and FERPA requirements for non-directory student records are met, all program evaluation and assessment data must be stored in such a way that responses are not associated with individual names or SSNs. Linkage files containing the association of protected data to individuals must be placed in different directories and with different naming conventions to obscure the connection, and must be permanently deleted when no longer needed.

A student may file a directory exclusion to prevent disclosure of public information. For this reason, student public information must not be stored on local servers unless updated daily.

VIII. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the Provost is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every two years or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer and Information Security Officer.