Augusta University
Policy Library

Data Management and Classification

Policy Owner: Information Technology Support and Services

POLICY STATEMENT
The Augusta University data governance and management structure is responsible to implement policies and procedures to effectively manage and provide necessary access to institutional data, while ensuring the confidentiality, integrity and availability of the information.

This policy defines a structured and consistent process to obtain necessary data access for conducting Augusta University operations (including administration, clinical, instructional and research), identifying the relevant mechanisms for delegating authority to accommodate this process at the unit level while adhering to segregation of duties and other best practices, as well as defining data classification and safeguards in compliance with existing laws, rules, and regulations.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☐ Vendors/Contractors ☐ Visitors
☒ Other: Agents acting on behalf of the University and Business Associates and volunteers

DEFINITIONS
Data Categories: This policy requires that all institutional data be classified into one of the following categories as defined by the data stewards.

Unrestricted Data has no access restrictions and is available to the general public. (Example: Information on the public web site).

Restricted Data is not legally protected, but should not be made public and should only be disclosed under limited circumstances. Users must be granted specific authorization to access since the data's unauthorized disclosure, alteration, or destruction may cause perceivable damage to the institution.

The following are examples of restricted data elements:

- Non-directory information identifiable to an individual (including students, staff, faculty, trustees, donors, and alumni), including but not limited to, dates of birth, driver's license numbers, employee and student id numbers, license plate numbers and compensation information.

- The institution's proprietary information, including but not limited, to intellectual research findings, intellectual property, financial data, and donor and funding sources.

Regulated Data has a legal obligation not to disclose. These data elements require the highest levels of restriction due to the risk or potential harm that will result from disclosure or inappropriate use.

The following are examples of confidential data elements:

- Data not disclosed under the Georgia Open Records Act or the Georgia Open Meetings Act
- All regulated data protected under the following, but is not limited to:
- Family Educational Rights and Privacy Act of 1974 (FERPA) protected
- Gramm-Leach-Bliley Act (GLBA) protected
- Georgia Personal Identity Protection Act (GPIPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI)

Data access is the process of being granted authorization to interact with data at a level that includes, but is not limited to, read, write and modify.

Data trustees are Augusta University executives who have overall responsibility for all the data sets maintained by the units reporting to them. Institutional data trustees consist of the Provost, other Vice-Presidents and the Chief Information Officer (CIO). Individually the data trustees are accountable for all the data sets within their division. The CIO has the additional responsibility for ensuring an adequate and appropriate technical infrastructure is in place to support the data needs of the institution across all divisions.

Responsibilities:

- Ensures that institutional data resources are used in ways consistent with the mission of Augusta University
- Responsible for the appointment and accountability of data stewards

Data stewards, designated by the data trustees, are senior level officials who have planning and policy responsibilities for data in their functional areas. Data stewards, or their designees, are responsible for recommending policies, and establishing procedures and guidelines concerning the accuracy, privacy and integrity of the data subsets for which they are responsible. Individually, data stewards act as advisors to the data trustees and have management responsibilities for data administration issues in their functional areas. They have overall responsibility for the data in the subsets overseen by all their designated data managers.

Responsibilities:

- Interprets and implements federal, state and Augusta University policies, standards and guidelines.

- Ensures data quality and data definition standards are met.
- Identifies the privacy level, such as unrestricted, restricted, or confidential/regulated, for the data subsets.
- Establishes authorization procedures to facilitate appropriate data access as defined by campus data policy and ensuring security for that data.
- Resolves issues related to stewardship of data elements that cross multiple units or divisions. For example, Social Security number may have more than one data steward since it is collected or used in multiple systems, such as financial, human resources, and student systems.
- Develops standard definitions for data elements, including those that cross multiple units or divisions. For example, there should either be a single definition of “full-time employee” or new data elements should be created for each unique definition.
- Performs an annual recertification of user access for information systems that contain restricted and/or confidential/regulated data.

Data managers, designated by the data stewards, are generally operational managers within a functional area overseeing the data for a particular subject area. Data managers have day-to-day responsibility for managing administrative processes and establishing business rules for the transactional systems. They have operational responsibility for the data management activities related to the collection, maintenance, protection, and dissemination of data in their functional areas. The data manager may authorize operational tasks to be performed by data users outside the units that report to the data manager. The data managers are accountable for the data subsets they manage, whether the data are collected or maintained directly by the data manager (or their staff), by data users in other units or by external sources.

Responsibilities:

- Reviews and approves access requests.
- Determines the type of access given to an information system’s roles.
- Assures compliance with federal, state and institutional regulations regarding the release of, responsible use of, and access to, data.
- Trains Augusta University users in relevant regulations and proper understanding of data.
- Documents data definitions for each data element within the domain of their operational unit(s).
- Communicates any data definition or database changes to the appropriate data custodian.
- Ensures the accuracy, privacy and integrity of the data they manage.
- Assists in the design of data warehouse structures that contain data from their subject areas.

Data users are Augusta University employees who have been granted authorization by the data managers to access institutional data. Authorization is granted for a specific level of access, as defined by the data management policies, solely for the conduct of institutional business.

Responsibilities:

- Follows the policies and procedures established by the data stewards for responsible use of the Augusta University data. Using institutional data only as required to conduct Augusta University business.
- Ensures the privacy of data by viewing and storing data, and the information derived from data, under secure conditions.
- Ensures accuracy and timeliness of the data they enter or update.
- Collects, prepares, enters or maintains data for the authorized unit(s), if authorized by the data manager.

Data Custodians are Augusta University employees who have administrative and/or operational responsibility over institutional data. In many cases, there will be multiple Data Custodians. An enterprise application may have teams of Data Custodians, each responsible for varying functions.

Responsibilities:

- Understanding and reporting on how institutional data is stored, processed and transmitted by Augusta University and by third-party agents of the University.
- Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of institutional data.
- Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of institutional data.
- Provisioning and de-provisioning access to institutional data as authorized by the Data Steward and/or Security Authority.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of institutional data.

Security Authority is responsible for requesting access within a department to Augusta University/AUHS information systems.

Responsibilities:

- Request, revoke, and transfer access and permissions for various Augusta University/AUHS clinical and administrative systems.
- Notify Human Resources (HR) if a department head perceives that a terminating employee may pose some threat to systems or data. ITS will work with HR to terminate all access immediately.
- Manage access for any external entities doing business with your department – e.g. contractors, vendors, temporary employees, interns, volunteers and research collaborators.
- Responsible for submitting other access request for items such as non-birth right departmental share access, access to terminated employee mailboxes, or access to a secure share where the previous folder owner is no longer with the organization.

Institutional Data is data that provides support to, and meets the needs of, units of the institution. Examples of institutional data include, but are not limited to, many of the elements

supporting financial management, student curricula, payroll, personnel management, and capital equipment inventory.

Information may be considered institutional data if it satisfies one or more of the following criteria:

1. Data used for planning, managing, reporting, or auditing a major administrative function;
2. Data referenced or used by a participant organization to conduct organization business;
3. Data included in an official participant organization administrative report; or,
4. Data used to derive an element that meets any of the criteria above.

Family Educational Rights and Privacy Act of 1974 (FERPA) protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US law designed to provide privacy and security standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

Protected health information means individually identifiable health information that is:

i. Transmitted by electronic media;
ii. Maintained in electronic media; or
iii. Transmitted or maintained in any other form or medium.

Protected health information excludes individually identifiable health information in:

i. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
ii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
iii. Employment records held by a covered entity in its role as employer."

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

Georgia Personal Identity Protection Act (GPIPA) is an effort to protect individuals from the growing threat of identity theft caused by data breaches, the Georgia General Assembly passed the Georgia Personal Identity Protection Act

A GPIPA Event is the combination of a person's first name (or initial) and last name, plus one or more of the following: (i) social security number; (ii) driver's license number; (iii) state identification card number; (iv) account number; (v) credit card number; (vi) debit card number; (vii) account passwords;(viii) PINs; or (ix) other access codes. Items (iv), (v), and (vi) only apply if the account number could be used without additional access codes. 14

Gramm-Leach-Bliley Act (GLBA) provides limited privacy protections for private financial information. Additionally, the GLBA codifies protections against pretexting, the practice of obtaining personal information through false pretenses and implements rules concerning

financial privacy notices and the administrative, technical and physical safeguarding of personal information.

PROCESS & PROCEDURES

Data Access Request

1. The Departmental Security Authority (SA) receives a request from a requesting supervisor of workforce member(s) who has an authorized need for access to data.
2. The SA will vet the workforce member's authorization for data access through a documented approval process.
3. If the access request is validated by the SA, the SA places the request within Information Technology Services' (ITS) work management system for the access to be granted.
4. ITS will receive the request, fulfill the requested access and provide information back to the SA on its completion status.
5. The ITS Service Desk is available as a resource for any troubleshooting needs at 706-721-4000.
6. Data access privileges can be revoke by the SA by placing a request into ITS' work management system, if they are no longer necessary.
7. Upon termination, the SA is responsible for submitting a "revoke all" request within the ITS work management system to remove all privileges to information systems.
8. The Information Security Office, in collaboration with the Enterprise Privacy Officer and the Department of Human Resources, reserves the right to remove data access at any point.

REFERENCES & SUPPORTING DOCUMENTS

Augusta University Confidentiality Statement

FERPA Annual Notification

Privacy of Health Information (HIPAA) Policy

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

President, Augusta University and CEO, AU Health System Date: 06/20/2017