Augusta University
Policy Library

Data Management and Classification Policy

Policy Manager: Chief Information Security Officer

POLICY STATEMENT

This policy applies to all employees and staff of Augusta University (AU), hereinafter referred to collectively as "AU". This policy applies to all duties of AU employees and staff performed within the scope of their employment at any site of the AU. AU is committed to protecting Protected Health Information (PHI), electronic Protected Health Information (ePHI), and/or other sensitive information (SEI) by implementing physical security standards within facilities and within areas of a facility that contain or provide access to SEI, PHI, PCI, FERPA or ePHI.

This policy is in accordance with requirements of the University System of Georgia, USG IT Handbook.

The purpose of this policy is to identify the different types of data and to establish a framework for classifying and managing institutional data based on its level of sensitivity, value, and criticality to AU.

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: Any other individual with a relationship to AU that may create, use, disclose or access data owned or managed by Augusta University

DEFINITIONS

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.

The **Family Educational Rights and Privacy Act (FERPA)**: (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
See https://www.augusta.edu/registrar/documents/ferpadefinitions.pdf

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.
See https://www.augusta.edu/compliance/privacy/hipaa.php

Georgia Open Records Act (ORA): is a series of laws guaranteeing the public access to public records of government bodies. Public records are those documents generated by individuals or groups in public office in the course of public service.

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 involves the use of the combination of a person's first name (or initial) and last name, plus one or more of the following when not encrypted or redacted: (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.

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.

POLICY

1. Classification of Data

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** is information maintained by AU that is not exempt form disclosure under the provisions of the ORA or other applicable state federal laws. Some level of control is required to prevent unauthorized modification or destruction of public information.
- **Sensitive Information** is information maintained by AU that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of AU financial transactions and regulatory actions.
- **Confidential Information** is maintained by AU. This information is exempt from disclosure under the provisions of the ORA or other applicable state or federal laws.

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. Please refer to the *USG IT Handbook* for further information and guidance.

1. Notice-triggering personal information - specific items or personal information (name plus Social Security Number, driver's license/Georgia identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person.

2. Protected Health Information - individually identifiable information created, received, or maintained by such organizations as health care payers, health care providers, health plans, and contractors to these entities, in electronic or physical form. Laws require special precautions to protect from unauthorized use, access, or disclosure.

3. Electronic Health Information - individually identifiable health information transmitted by electronic media or maintained in electronic media. Federal regulations require state entities that are health plans, health care clearinghouses, or health care providers conducting electronic transactions ensure the privacy and security of electronic protected health information from unauthorized use, access, or disclosure.

4. Personal Information for Research Purposes - personal information requested by researchers specifically for research purposes. Releases may only be made to AU in accordance with the provisions set forth in the law.

5. Personally Identifiable Information (PII) - any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the institution. Some PII is not sensitive, such as the PII on a business card, while other PII is considered Sensitive Personally Identifiable Information (Sensitive PII), as defined below.

6. Sensitive Personally Identifiable Information (Sensitive PII) - personally identifiable information that if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, such as a Social Security number or alien number (A-number). Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if compromised.

2. Management of Data

Data Owner Augusta University is responsible for all data read, created, collected, reported, or deleted by offices of the organization. The heads of Augusta University, the president, chief executive officer, Chancellor, or other identified head of AU is identified as the data owner. AU has the responsibility for the identification, appointment and accountability of data trustees. Data owners will inform the Data Trustees Committee of their data trustee appointments including office, name and contact information.

Data trustees

Data trustees are designated by the data owner and are executives of AU who have overall responsibility for data read, created, collected, reported, updated, or deleted in their data area(s). AU data trustees have overall responsibility for accuracy and timeliness of submission of data to the Data Trustees Committee. These positions and offices normally report directly to the entity data owner.

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 trustees will inform the AU Data Trustee Committee of their data steward' appointments, including office, name and contact information of the incumbent;
- Participate as a member of the Data Trustees Committee
- Communicate unresolved concerns about data (such as data quality, security, access, etc.) to the data owner.

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 to the data trustees, 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 stewards.

Responsibilities:

- Interprets and implements federal, state, 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 AU 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 AU 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 AU employees who have administrative and/or operational responsibility over institutional data. In many cases, Data Custodians are members of the information technology team.

Responsibilities:

- Understanding and reporting on how institutional data is stored, processed and transmitted by AU 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 (SA) is responsible for requesting access within a department to AU information systems.

Responsibilities:

- Request, revoke, and transfer access and permissions for various AU 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. IT 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.

PROCESS & PROCEDURES

Data Access Request

1. 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 (IT) work management system for the access to be granted.
4. IT will receive the request, fulfill the requested access and provide information back to the SA on its completion status.
5. The IT Service Desk is available as a resource for any troubleshooting needs at 706-721-7500.
6. Data access privileges can be revoked by the SA by placing a request into IT 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

Confidentiality Statement

USG IT Handbook https://www.usg.edu/information_technology_services/it_handbook/

RELATED POLICIES

Acceptable Use of Information Technology

Cybersecurity Risk Management Policy

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/2/2021

President, Augusta University Date: 6/2/2021