Data Access Policy

I. POLICY STATEMENT

All Auburn University data, whether maintained in central databases or maintained by other data systems, including personal computers, remains the property of Auburn University and is covered by all Auburn University data policies. Access to and use of data will only be approved for legitimate Auburn University business.

By law and University policy, certain confidential and operational data is sensitive and may not be released without proper authorization. Users must adhere to any applicable federal and state laws as well as Auburn University policies and procedures concerning storage, retention, use, release, and destruction of data.

II. POLICY PRINCIPLES

The purpose of this Data Access Policy is to ensure the security, confidentiality and appropriate use of all data which is processed, stored, maintained, or transmitted on Auburn University computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy is intended to serve as a general overview on the topic and may be supplemented by other specific policies required by law such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Gramm Leach Bliley Act (GLBA).

Data captured and maintained at Auburn University is a valuable university resource. While this data may reside in different database management systems and on different machines, this data, in aggregate, form one logical university resource. The Central Administrative Systems contain data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

The Data Access Policy applies to all individuals who have access to Auburn University computer systems and networks, including but not limited to all Auburn University employees and students who may or may not have been granted access to confidential and operational data during the normal course of their employment with Auburn University. It applies not only to stored information, but also to the use of the various computerized systems and computerized programs used to generate or access data**,** the computers which run those programs (including workstations to which the data has been downloaded), and the monitors and printed documents that display data.

Access to Auburn data should reasonably comply with the concept of minimum necessary/least privilege.

Access to information will only be provided to users based on business requirements, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be for a valid business need and approved by the appropriate supervisor and/or owner of the application system or data.

III. EFFECTIVE DATE

Adopted: 04/13/2007
Revised: August 31, 2017
Revised: September 16, 2019

IV. APPLICABILITY

This policy applies to all Auburn University employees, students, and agents.

V. POLICY MANAGEMENT

***Responsible Office*:** Office of the Chief Information Officer

***Responsible Executive*:** Chief Information Officer

***Responsible Officer*:** Chief Information Security Officer

VI. DEFINITIONS

Access Control Administrator – An Auburn professional position in the Office of Information Technology, Distributed IT, or departmental personnel who are responsible for processing approved requests.

Oversight Committee – A University committee with membership representative of all Central Administrative Systems areas. This committee provides oversight for the entire Central Administrative Systems and interacts as needed with the modular steering teams (i.e., HR Steering Team, Student Steering Team, Finance Steering Team, Financial Aid Steering Team, etc.).

Minimum Necessary/Least Privilege - A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges, view privileges, data download privileges) to the minimum necessary to perform their jobs.

Central Administrative Systems – any centrally managed systems that support the administrative functions of Auburn University.

Data Owners – Executive level employees who are responsible for determining who should have access to data within their jurisdiction and what those access privileges should be.

Data Custodians – Individuals designated by the Data Owner that oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area.

Data Stewards – University employees typically at the director level that are responsible for the administration of specific user access within their business area(s).

Data Users – Individuals who access data in order to perform their assigned duties or fulfill their role in the Auburn University community.

Data Access Controls - Access controls based on data classifications as specified in the Auburn Data Classification Policy will be considered in developing access controls for query (view) and modify access.

Query (Read Only) Access – Access enabling the user to view, but not update data.

Modify Access – Access enabling the user to both view and update data.

VII. POLICY PROCEDURES

Data Administration

Division/department heads are responsible for ensuring a secure office environment regarding all data. Division/department heads will review the data access needs of staff as it pertains to their job functions before requesting access.

Sensitive and administrative data (regardless of how collected or maintained) will only be shared among those employees and agents who have demonstrated a job related need to know.

Access to Data

Below are the requirements and limitations for all Auburn University divisions/departments to follow in obtaining permission for access to data.

Division/department heads or their designee must request access authorization for each user under their supervision. They will also assure termination of access when a user leaves the department either by transfer, retirement, or leaving Auburn. Approved requests will be forwarded to the appropriate Security Administrator for processing.

Secured Access to Data

Role-based access control (RBAC) (classifications) will be established based on job function. Specific capabilities will be assigned to each role. Each user will be assigned a r o l e . Some users may be assigned several roles depending on specific needs identified by their division/department head and approved by the Data Steward(s).

The use of generic accounts is prohibited for any use that could provide access to confidential or operational data.

Periodic Access Review (PAR)

The Data Owners will periodically review individual user access to ensure the continued need and appropriateness of the data access.

VIII. SANCTIONS

Deliberate disregard of this policy or principles may result in disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

None

X. INTERPRETATION

The Chief Information Security Officer or designee has the authority to interpret the policy and its application.

FINAL APPROVAL: Executive VP, Provost,
Banner Executive Committee