Core Administrative Systems Access and Security Policy

I. POLICY STATEMENT

By law and University policy, certain data is confidential 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.

All Auburn University Core Administrative data, whether maintained in a central database or captured 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 should be approved only for legitimate Auburn University business.

Data from Auburn University systems and databases will be accessed and updated only with standard system supplied facilities.

II. POLICY PRINCIPLES

The purpose of this Core Administrative System Access and Security 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.

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

The Core Administrative System Access and Security 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 or endpoints to which the data has been downloaded, and the monitors and printed documents that display data.

III. EFFECTIVE DATE

Adopted: 4/13/2007; Revised: August 31, 2017

IV. APPLICABILITY

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

V. POLICY MANAGEMENT

Responsible Office: Office of Chief Information Officer
Responsible Executive: Chief Information Officer
Responsible Officer: Chief Information Security Officer

VI. DEFINITIONS

Administrative Data - Any data that resides on, is transmitted to, or extracted from any Core Administrative Systems, including databases or database tables/views, file systems and directories, and forms.

Security Administrator - An IT professional position in the Office of Information Technology responsible for processing approved requests.

Oversight Committee - A University committee with membership representative of all Core Administrative Systems areas. This committee provides oversight for the entire Core 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.).

Core Administrative Systems - any centrally managed systems that support the administrative functions of Auburn University.

Data Owners - Data Owners are responsible for determining who should have access to data within their jurisdiction, and what those access privileges should be. Responsibilities for implementing security measures may be delegated, though accountability remains with the owner of the data.

Area of Responsibility	Data Owners
Student Data	Provost
Student Financial Aid Data	Executive Vice President
Finance Data	Executive Vice President
Human Resources Data	Executive Vice President, Vice Chancellor AUM
Faculty Academic Records	Provost
Accounts Receivable	Executive Vice President
Procurement & Payment Services	Executive Vice President

Data Custodians - Data Custodians oversee data management functions related to the capture, maintenance and dissemination of data for a particular operational area. They are responsible for the general administration of user access to data within their area(s) of responsibility. Data Custodians are appointed by the respective Data Owner.

Area of Responsibility	Data Custodian(s)
Student Data	Associate Provost for Undergraduate Studies; Dean of Enrollment Mgmt; Dean of the Graduate School

Financial Aid Data	Associate VP for Business & Finance; CFO
Finance Data	Controller
Human Resources Data	Associate VP for Business & Finance; CFO Assistant VP for Human Resources; Vice Chancellor AUM
Faculty Academic Records	Provost
Accounts Receivable	Controller
Procurement & Payment Services	Associate VP for Business & Finance

Data Stewards - University Directors (typically at the level of Registrar, Executive Director of Benefits, Payroll and Records, Executive Director of Student Financial Services, etc.) that are responsible for the administration of specific user access within their business area(s). Data Stewards are appointed by the respective Data Custodian.

Data Users - Data users are individuals who access data in order to perform their assigned duties or fulfill their role in the Auburn University community.

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.

This access is limited to users directly responsible for the collection and maintenance of data.

VII. POLICY PROCEDURES

Data Administration

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

Administrative data (regardless of how collected or maintained) will only be shared among those employees who have demonstrated a job related need. Although Auburn University must protect the security and confidentiality of data, the policies allowing access to data must not unduly interfere with the conduct of Auburn University business.

Access to Administrative Data

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

Division/department heads or their Administrative Computing Coordinator must request access authorization for each user under their supervision. They will also assure termination of access when a user leaves the department. The appropriate Data Steward(s) will review requests and approve or deny. Approved requests will be forwarded to the appropriate Security Administrator for processing.

Secured Access to Data

Security classifications will be established based on job function. Specific capabilities will be assigned to each security classification. Each user will be assigned a security classification. Some users may be assigned several security classifications 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.

VIII. SANCTIONS

Deliberate violation of this policy will be considered a Group I infraction under the Auburn University Personnel Policies and Procedures Manual and is subject to disciplinary action, up to and including dismissal.

IX. EXCLUSIONS

If access is denied an appeal may be made in writing to the Data Owner.

X. INTERPRETATION

FINAL APPROVAL: Executive VP, Provost, Banner Executive Committee
Dated 04/14/2007