Enterprise System Access and Data Stewardship Policy

I. Purpose

The purpose of the Albany State University Enterprise System Access and Data Stewardship Policy is to provide guidelines for the management of and access to data, which are critical to the administration of the University. This policy will describe the roles and responsibilities of stewardship for University Information and procedures for establishing access to University Information.

II. Policy

It is the policy of Albany State University that all University Information be used with appropriate and relevant levels of access and with sufficient assurance of its integrity in compliance with existing laws, rules, and regulations. The goal of this policy is to provide reasonable procedures for the University community to follow so that the value of data as a University resource is increased through its widespread and appropriate use.

III. Scope

This policy applies to **UNIVERSITY INFORMATION** only (as defined in Section IV) and is intended to improve access to these data by employees for conducting University business. This policy also applies to all employees with access to enterprise systems that contain such information. In all cases, applicable statutes, rules, and regulations that guarantee either protection or accessibility of institutional records will take precedence over this policy. While this policy is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microform, and video, as well as the content of confidential meetings and conversations. This policy does not apply to notes and records that are the personal property of individuals in the University community and is not directed to data whose primary purpose is scholarly (e.g., instructional material, research notes).

The scope of this policy is to have broad application, particularly with respect to data and information resources, which have impact for institutional operation. Data that may be managed locally may yet have significant impact if it is used in a manner that can impact University operations. It is expected that the intent of this Enterprise System Access and Data Stewardship Policy be extended in analogous manner to all data and information used at all operational levels of the University.

IV. Definition of Terms

Enterprise systems are software and database management systems that provide core services used across the institution and on which other applications often are dependent.

Unrestricted Data is considered to be data that does not have access restrictions and is available to the general public.

Sensitive Data is considered data for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the University.

Confidential Data includes information whose improper use or disclosure could adversely affect the ability of the University to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), or data not releasable under the Georgia Open Records Act or the Georgia Open Meetings Act.

University Information—A data element is considered **UNIVERSITY INFORMATION** if it provides support to and meets the needs of units of the University. Examples of **UNIVERSITY INFORMATION** include, but are not limited to, many of the elements supporting financial management, student curricula, payroll, personnel management, and capital equipment inventory. Data may be considered **UNIVERSITY INFORMATION** if it satisfies one or more of the following criteria:

1. It is used for planning, managing, reporting, or auditing a major administrative function;
2. It is referenced or used by an organizational unit to conduct University business;
3. It is included in an official University administrative report;
4. It is used to derive an element that meets the criteria above.

V. User Definition and Authority

A. Enterprise System users: All personnel of Albany State University who have access to an Enterprise system will be considered as having a data stewardship access level in one of the three (3) categories below:

i. ***Data users*** are the academic and administrative users expected to access University Information only in their conduct of University business, to respect the confidentiality and privacy of individuals whose records they access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws, rules, regulations, or policies.

ii. ***Data stewards*** are responsible for defining and documenting a single set of procedures by which users may request permission to access sensitive data and which shall govern their use of such data. Documentation of the data elements and their appropriate use is the responsibility of the data stewards.

iii. **Enterprise System Managers are** responsible for all the organization's enterprise system initiatives, for enterprise system standards, and for enterprise system tools. The enterprise system managers work in conjunction with the data stewards and data users to ensure smooth operation of all enterprise systems the University relies upon.

iv. ***Data Administration Steering Committee*** is responsible for working with the Data Stewards and enterprise system managers in educating the University community about University Information, its use, restrictions, and consistency.

B. Functional Data Classifications -- Data stewards of the University are the senior managers who are in charge of the functional areas of the

University. These functional areas are defined by the primary University purpose served by the data. Due to extensive interaction across functional units, functional classification may not necessarily follow organizational lines of authority. A functional unit may be given authority for data that is shared by many other organizational units.

C. Authority of Data Stewards: Data stewards will work together to define a single set of procedures for requesting access to sensitive elements of University Information and to document these data access request procedures. Data stewards also have responsibility for documenting the meta-data about their data so that users are aware of the definitions, restrictions, or interpretations, and other issues which ensure the correct use of the data.

VI. Requesting Data Access:

Data stewards of the University are responsible for initiating and approving all requests for the data access users. The process includes the following steps:

A. Requests for access for all data users must be made in writing by the data user's supervisor to the Chief Information Officer (CIO) for Albany State University. Such requests must include approval by the requestor's supervisor or management and should be **specific** as to the data needed and the purpose for accessing the data.

B. Upon approval by the CIO, the request will be forwarded to Database Administrator for creation of the access logins.

C. The requestor and the data user will be notified of access and will be provided a copy of this Data Stewardship & Access Policy and the relevant functional guidelines as to use and restrictions of the data (such as the Family Educational Rights and Privacy Act regulation.)

D. If training is needed before Access rights are granted, it is the responsibility of the data user to schedule, attend, and successfully complete all training required in order to receive their access rights and logins.

E. All data access will be reviewed and renewed on an annual basis by each Data Steward and the Office of Information Technology to ensure that the access remains appropriate.

VII. Revocation of Data Access

A. Violations of Policies and Laws -- Access to Enterprise Systems can be suspended or lifted entirely for infractions of Albany State's Acceptable Use Policies, Faculty & Staff Handbook policies and procedures, or any other relevant user policies which govern the use of and access to the Enterprise System. This also includes, but is not limited to, violations of federal laws, such as FERPA and the Gramm-Leach-Bliley Act.

B. End-of-Affiliation – If the user resigns, is terminated, or in any way ceases affiliation with the University, the University will, at the time of termination, expire access to all enterprise systems to which the user has access. After a review by the data stewards and the CIO, the account may be subject to deletion by the data administrator.