ERP Sensitive Data Policy

I. PURPOSE

To protect Auburn University sensitive data from unauthorized disclosure and inappropriate use.

II. POLICY

It is the responsibility of each individual with access to sensitive data resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

- Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations than central servers.
- Access to computers that are logged into central servers storing sensitive data should be restricted (i.e. authenticated logins and screen savers, locked offices, etc.).
- Access to sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.
- All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.
- Copies of sensitive data resources should be limited to as few central servers as possible.
- Sensitive data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.).
- Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the appropriate University official.

III. APPLICABILITY

University wide - applies to all individuals who have access to sensitive data, including but not limited to social security numbers, credit card numbers, computer passwords, date of birth, driver license number and any personal information flagged for non-disclosure.

IV. RESPONSIBILITY

OIT and Colleges/Schools/Departments IT support staff assigned to provide system management for computers where sensitive data is stored.

Any employees who may encounter sensitive data as a routing part of their job, or who unintentionally encounter such data.

V. DEFINITIONS

Sensitive Data - any information that could cause an individual personal financial harm if disclosed and used improperly. Examples of sensitive data include but are not limited to social security numbers, credit card numbers, computer passwords, and any personal information flagged for non-disclosure.

VI. SANCTIONS

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

VII. INTERPRETATION

CIO – Executive Director, OIT, ERP Coordinator

FINAL APPROVAL: Executive VP, Provost, Banner Executive Committee

ADOPTED: 2/6/2007