ERP Data Protection Policy

Responsible Office: Office of Information Technology

I. PURPOSE
To ensure the security, confidentiality and appropriate use of all data 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.

II. POLICY
It is the responsibility and duty of any individual who has access to University computer systems and networks to protect University data resources in whatever form, from unauthorized modification, destruction or disclosure. Without limiting the forgoing, all individuals granted access to Auburn University Information Technology resources are expected to adhere to the following principles:

1. Refrain from any deliberate violation of University or departmental policy and/or any state or federal law governing information privacy and use.

2. Refrain from attempting to access confidential or proprietary data on Auburn University computer systems, or in any other manner, except when it is in keeping with the specific assigned duties as an Auburn University employee.

3. Appropriately maintain and protect the confidentiality of any data to which access has been granted, regardless of the method used to retrieve or display it.

4. Refrain from making any unauthorized alterations (add/change/delete) to any data which is accessible either through legitimate granted access or any incidental access.

5. Prevent the download, distribution, and installation of pirated software and copyrighted or proprietary materials for which the user has not acquired rights, and will strive to prevent the download, distribution, and installation of software and such materials without a valid license or the installation of a single user license on multiple machines.

6. Refrain from remotely or physically logging into or attempting to log into another user’s machine or attempt to access another user’s files without the individual’s permission, except when necessary in the course of performing specific assigned duties as an employee.
7. Refrain from attempting to compromise the security of the Auburn University network or devices attached to the network, except when it is necessary in the course of specific assigned duties as an employee.

8. Insure the proper disposal of all confidential or proprietary information in whatever form in accordance with University or departmental policy.

III. APPLICABILITY
University wide - applies to all individuals who have access to Auburn University data, 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 sensitive data during the normal course of their employment with Auburn University.

IV. RESPONSIBILITY
OIT and college/school/department system administrators and other employees with system administration responsibility for computers.

V. 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.

VI. INTERPRETATION
CIO – Executive Director, OIT, ERP Coordinator

FINAL APPROVAL: Executive VP, Provost, Banner Executive Committee

ADOPTED: 04/13/2007