MERCER UNIVERSITY	SECTION:

Policies and Procedures Manual
Department of Information Technology

SUBJECT:	EFFECTIVE:
Administrative Applications and Data Security Policy	**September 14, 2004**

PURPOSE: The purpose of this policy is to ensure the security of administrative information ***(Data)*** which is processed, stored, maintained, or transmitted on computing systems ***(Systems)*** and networks centrally managed by Information Technology, and to protect the confidentiality of that data. This policy is designed to protect data from unauthorized change, destruction, or disclosure, whether intentional or accidental.

Scope
Words in bold italics have specific meanings within this document, as described in the Definitions section, below, and determine the scope of the policy. This policy applies to any Information Technology employees (permanent or temporary) ***(Staff)*** who have access to data. It regulates the use of the systems and applies to all computer programs used to access data as well as the computers and terminals which run those programs including workstations to which the data has been downloaded.

Policy
It is the responsibility of IT staff to protect data from unauthorized change, destruction or disclosure according to University, campus or local guidelines, as well as any other regulations or laws which may apply. This policy governs all IT-maintained central administrative systems which provide access to data and defines the responsibilities of the staff who maintain or use those systems. It should be noted that, in general, IT is not the ***Data Owner,*** but is the ***Custodian of the Data.*** It is the owner who has the authority to grant or revoke access to data or systems which use data. It is IT's responsibility to implement specific procedures which enforce access authority and establish guidelines and standards for systems and data security under this policy. It is also IT's responsibility to establish and promulgate procedures for the dissemination of this policy. Each individual is responsible for carrying out his or her responsibilities under this policy.

Violation
Violations of this policy include, but are not limited to: accessing data or systems to which the individual has not been specifically given access; enabling unauthorized individuals to access the data; disclosing data in a way which violates applicable policy, procedure or other relevant regulations or laws; or inappropriately modifying or destroying data. Violations may result in access revocation, corrective action up to and including dismissal, and/or civil or criminal prosecution under applicable law. Recourse under this policy is available under the appropriate section of the employee's personnel policy or contract, or by pursuing applicable legal procedure.

Definitions:

- ***Custodian of the Data:*** the entity or office that is delegated by the data owner the responsibility of performing management functions for the data.
- ***Data:*** administrative information which is processed, stored, maintained, or transmitted on computing systems and networks centrally managed by IT.
- ***Data Owner:*** the entity or office that is authorized to collect and manage the data as official record.
- ***Staff:*** any IT employees (permanent or temporary) who have access to data.
- ***Systems:*** all IT maintained central administrative systems which provide access to data.