Title: Access to Information Resources and Data

Purpose: This document establishes the policy for setting up access to log into an application which contains sensitive and important university information. This policy addresses what information different application users can see and modify.

Scope: Applies to anyone requiring access to central institutional data which includes but is not limited to:

- Financial Records System Access
- Human Resources System Access
- Student Information System Access
- Alumni Development System Access

Policy: Data managers are responsible for granting access to the institutional data under their custodial care (see Policy #74). Furthermore, data managers will determine what level of access a granted user will receive.

Data managers will review Security Level Reports for accuracy and will notify ITS of adjustments that need to be made.

ITS is charged with making no changes to user access levels without approval by the appropriate data manager. ITS is further charged with making changes to user security as requested by Data Managers on a timely basis. Exceptions will be documented and held for review by the designated UNC Asheville Information Technology Security Officer.

Data users and managers are reminded that sharing passwords is strictly prohibited.

Definitions:

**Information Technology Security Officer** is a person or persons designated by the UNC Asheville CIO who can verify that accounts are set up in accordance with the data manager's directives. Current Information Technology Security Officers are Richard White and Robin Daugherty.

**Institutional data** is interpreted to be data which resides in centrally managed broad impact databases and supports the core business functions of the University.

**Security Level Reports** are produced daily and made securely available online to data managers.

Approved on: 10/02/2008
Next review: 10/02/2010