Policy No: 807
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Digital Access Security Policy

BACKGROUND

Unauthorized access to sensitive resources is a high level concern in the realm of information security. Most unauthorized access is attributed to people within the University. Damage that is caused may be intentional or accidental. Methods of managing digital access to sensitive resources are necessary means to help ensure that access to resources is only by authorized personnel.

POLICY

University information shall be stored in locations, as approved by the Chief Information Officer (CIO) designated by the appropriate administrative office that is custodian of the data. Access to that information shall be authorized or denied by the "data owner". The approved data custodian may use a limited number of administrative accounts for purposes of managing or troubleshooting the data store. The users of those accounts will be registered to the data owner's security contact and the CIO.

Data owners must use due care when authorizing access to data. Access should be authorized on an individual basis. Requests for accounts should go through procedures appropriate to the business process associated with the data.

DEFINITIONS

Data Owner – Administrative Office primarily responsible for the use and management of the data. A data owner may also be an individual responsible for the information stored on the machine to which they are responsible for.

Data Custodian –Person approved by the CIO or their designee to be responsible for the maintenance of the storage unit and facility.