

Policy No: 802

Area: Information Technology Services

Adopted: 8/6/2012

Information Security Operational Procedures Backup Policy

BACKGROUND

Data can be destroyed by system malfunction, accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. The ongoing availability of university data is critical to the operation of the institution. In order to minimize any potential loss or corruption of this data, units responsible for providing and operating category A and B administrative applications are responsible for ensuring data is adequately backed up by establishing and following an appropriate system backup procedure.

POLICY

Each unit responsible for providing and operating category A or B administrative applications must develop in cooperation with the Division of Information Technology & Services (ITS), and approved by the Chief Information Officer (CIO), a plan for periodic backup. The frequency of these backups, retention location, and the retention timeframes of each will be dependent on the criticality and volatility of the data residing on each system.

DEFINITIONS

ADMINISTRATIVE APPLICATION TYPES

- A -Applications which collect and/or update university data.
- B -Applications which use university data for "official" purposes outside of the local unity, but which do not collect and/or update university data.
- C -All other applications: those which deal with data for local purposes only.

UNIVERSITY DATA -Administrative Data and/or Information are the collection of data elements which are relevant to the operations, plans, or management of more than one GCSU unit or are reported on or used in "official" administrative university reports.

SYSTEM BACKUP - A documented procedure for copying applications software and data files that reside on computer disks to a portable medium (such as tape or diskette) or to a medium that is physically remote from the originating system.