Computer Systems Backup Policy

1. **Introduction**
   This policy on computer systems backups is based on *Security Backup Files as Public Records in North Carolina: Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files* published by the Archives and Records Section of the N.C. Division of Historical Resources.

2. **Policy**
   Brunswick Community College requires that computer systems maintained by Information Technology Services (ITS) be backed up periodically and that the backup media is stored in a secure off-site location (Bolivia, NC BB&T). The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files. The systems backups will consist of regular full and incremental backups. Although security backup files are public records according to G.S. 121-2(8) and 132-1, systems backups are not intended to serve as an archival copy or to meet records retention requirements.

   Systems backups will be performed on a regular schedule as determined by the Information Technology Services department. Backups will be stored in a secure off-site location based on the schedule listed below.

3. **Procedures**
   The Computer Systems Backup Policy provides guidelines for establishing backup procedures. Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

   a. Daily full systems backup are performed and stored on a backup server.
   b. A full systems backup will be performed weekly. Weekly backups will be saved for a full month.
   c. The last weekly backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled for other uses or destroyed.
   d. Monthly backups will be saved for three years, at which time the media will be recycled or destroyed as the data will have been archived according to the retention policy.
   e. Snapshots are copied to the backup server daily of changes made since last snapshot.
   f. All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
   g. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
   h. Periodic tests of the backups will be performed to determine if files can be restored.
   i. A complete list of network devices and associated information is kept in the College's vault in A113 as well as a list of all server and network equipment login and password information.

Approved by Brunswick Community College Board of Trustees
June 9, 2010
June 28, 2013