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 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 differential 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.

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 backups are performed beginning at midnight and stored on a backup server, Unitrends Cloud Services, and on an external hard drive for the previous year(s) at BB&T.
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, after payroll completion will be saved as a monthly backup. All other weekly backup storage space will return to backup cycle.
d. Monthly backups will be saved for seven (7) years, at which time the media will be recycled or destroyed.
e. Synchronization is scheduled every 2 hours beginning at 6 am each day and continues until 10pm each night for all files that have changed since last sync. No data is more than 2 hours young.
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 (BB&T).
g. All backup media that is not re-usable shall be thoroughly destroyed by using an arbor press and completely breaking all platters in the hard drive.
h. Periodic tests of the backups will be performed to determine if files can be restored and results documented using TrackIt software.
i. A complete list of network devices and associated information is kept in the vault a BB&T 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; April 4, 2016