Banner Student Information System (Banner) Backup Process

1.0 Purpose
The purpose of this document is to provide an overview of the Banner Student Information System (Banner) Backup Process.

2.0 Scope
The scope of the document and process apply to Information Technology Services System Administrators, Banner Database and Applications Administrators, the Banner Security Administrator, and Banner Data Custodians.

3.0 Backup Process

3.1 System Administrators
System administrators for the Banner System ensure that backups occur on the following standard schedule, per saveset: 1) Incremental backups are performed every other day; and 2) A full backup weekly. These backups are considered “system” backups and include backup up of the operating system, applications, and data.

The savesets are written or cloned and stored at the following locations:
- Tape library in the Campus Data Center in the Boyd Building at the University’s main campus
- Tape library in the Syncglobal colocation facility located in Breman, Georgia
- Stored in locked media transport containers with American Document Securities, Carrollton, Georgia
- Disk-based backup on the Data Domain appliance in the Boyd Building at the University’s main campus

System administrator backups of the Banner system mainly for restoration in the event of a catastrophic failure of the Banner system or if there is a need to “rollback” or “back out of” an operating system update/upgrade or an application installation/upgrade.

3.2 Database Administrators
The database administrator ensures that the Banner database is backed up to disk on the Banner server on a daily basis. Two (2) backups are kept on the database server before eventually being overwritten and “rolled off” of the server. A copy of the most current database backup is copied and synchronized to the Syncglobal colocation in Breman, Georgia.

Backups maintained by the database administrator are most useful for “immediate” restoration or “rollbacks” of the database.

3.3 Physical Security
Physical access to media, servers, network switches, and data facilities is controlled and monitored. Access to hosts storing, performing, or accessing backup data is controlled and monitored. Network communication between servers using student data and the backup hosts occurs entirely within secured data facilities.

Last Modified: 11/20/2012 – Mardel Shumake