Purpose:
To specify requirements of backups of systems which contain information necessary to maintain and resume normal business. These backups would be used in case of an emergency or other occurrence that results in the loss, destruction, theft or corruption of such information.

Scope:
All UF HSC information systems that contain information needed to continue normal business and/or have been designated as “crucial,” per Standard CP0002.02.

Reference:

Policy:
1. A retrievable exact copy of all UF HSC data (whether these data are deemed crucial, Restricted or not) is to be maintained on a written schedule determined to be appropriate by the Unit Information Security Administrator of each individual Unit in conjunction with the owner’s designee or delegate of the data. This determination shall be based on the nature of the data. Backup data should be moved to a secure off site location in a timely manner.
2. The Units are responsible for establishing the written procedures necessary to back-up and restore any data and providing coverage for the systems they are responsible for maintaining in a manner consistent with good business resumption planning. This should then be attached to the contingency plan.
3. These written procedures should include periodic testing to insure data can be retrieved and restored from the backups and normal business operations can be resumed.
4. A retrievable exact copy of all crucial and/or restricted data must be obtained before moving any equipment.
5. Each Unit will establish written procedures instructing personnel on how to access electronic backup data during an emergency.
6. On a periodic basis, or as needed in response to environmental and/or operational changes within the Unit, each Unit will review and update written backup procedures.

7. Backup media must have at a minimum the following identifying criteria:
   a. IT Resource name.
   b. Creation Date.
   c. HSC Contact Information.