Policy: TS0001	Category: Technical Security	Version Date: 02/22/2010
Title: **Key Person Dependency – Information Technology Personnel**		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 07/15/2009
Reviewer: HSC Chief, Information Security		Next Review: 07/15/2012

Purpose:

To ensure that all areas of responsibility are covered by trained (as determined by the Unit Information Security Administrator) Information Technology personnel.

Scope:

All UF HSC Information Technology positions and areas of responsibility that are needed to continue and maintain normal business processes and while operating in contingency mode.

Reference:

1. Policy CP0002: Contingency Plan

Policy:

1. It is the responsibility of the Dean, Director, or Department Chair to ensure that Information Technology functions that are deemed essential by the Unit Information Security Administrator (ISA) and Unit Information Security Manager (ISM) to maintain normal business processes are appropriately staffed and that a clear chain of command exists.
   a. Backup staff who will be used to cover these functions must be formally designated and have appropriate skills, expertise and training.
   b. Contact information must be maintained for both regular and backup staff.
2. Documentation of both system functional capabilities and technical architecture must be developed and maintained.
3. The Unit ISA must notify the Dean, Director, or Department Chair of the minimum personnel required to operate while in contingency mode, as referenced by Policy CP0002.