UF UNIVERSITY of FLORIDA
Information Technology

POLICY

Policy: GP0004	Category: General Provisions	Version Date: 2/1/2017
Title: Information Security Considerations re: Termination		Effective Date: 2/15/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/1/2017
Review Resp: HIPAA Security Officer		Next Review: 2/1/2020

Purpose:

To establish policy regarding information security concerns when an employee or business partner is terminated or changes association with the University. This policy is subordinate to the University of Florida Rules and supplements the policies and procedures of the University of Florida Human Resource Services and the Office of the Provost and Academic Affairs.

Scope:

This policy applies to all UF HSC individuals and Units that have been granted access to any Information Asset of UF HSC Information and Computing Environment, including, but not limited to UF HSC faculty and staff, volunteers, students, and third parties, and to all other users of Protected Health Information at UF.

References:

1. Data Classification Policy
2. University of Florida Human Resource Services policies and procedures: (http://hr.ufl.edu/working-at-uf/policies/)
3. University of Florida Regulations: http://regulations.ufl.edu/

Policy:

1. Voluntary termination: Generally includes voluntary separation or non-renewal of contract. Determination of termination as voluntary is at the discretion of the supervisor within the parameters of the University Rules.
    a. The employee's supervisor must notify the Unit Information Security Administrator or UFHealth IT Identity and Access Management Team within two workdays of the initial notice of termination. Notice to the administrator must include a listing of information assets to which the employee has access.
    b. The supervisor and the Unit Information Security Administrator will determine the timing and process for revoking access to information assets.
2. Involuntary termination: Generally occurs when an employee is being terminated for performance or for violation of University or Health Science Center policy/rules. Determination of termination as involuntary is at the discretion of the supervisor within the parameters of the University Rules.

a. The employee's supervisor must notify the Unit Information Security Administrator responsible for information security or UFHealth IT Identity and Access Management Team, in advance if possible or as soon as possible after the fact. Notice to the administrator must include a listing of information assets to which the employee has access.
b. Access to all electronic information assets must be disabled prior to or immediately upon termination. This includes disabling all user accounts.
c. The employee's supervisor must initiate a process for confiscating keys and other access devices as well as information assets classified as restricted, sensitive, or operational.
d. If the terminated employee fails to return keys, other access devices, or information assets classified as restricted or sensitive, the supervisor must notify the UF Information Security Office, Human Resources and the University Police Department (UPD).