

Standard: GP0003.06	Category: General Provisions	Version Date: 09/02/2009
Title: <b>Information Security Violation Levels</b>		Effective Date: 03/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 06/17/2009
Reviewer: HSC Chief, Information Security		Next Review: 06/17/2012

**Purpose:**

To delineate actions that may be taken by HSC Units in the case of disciplinary action, or the HSC Information Security Office in the case of suspension of computer or network access, for information security violations..

**Reference:**

1. Policy GP0002: Information Security Program Compliance

**Standard:**

<i>Degree</i>	<i>Description</i>	<i>Examples</i>	<i>Actions for Consideration</i>
1	<ul style="list-style-type: none"> <li>• Inadvertent Violation: A careless violation of UF HSC information security policy.</li> </ul>	<ul style="list-style-type: none"> <li>• Leaving a restricted or confidential document unattended where others could view it.</li> <li>• Failing to secure Restricted or confidential information, e. g., failing to lock a file cabinet or office door if required to do so by the Unit.</li> <li>• Failing to log off per the requirements of the Unit.</li> <li>• Sending email to the wrong recipient</li> <li>• Storing information in an inappropriate location.</li> <li>• Non-business related web surfing resulting in</li> </ul>	<ul style="list-style-type: none"> <li>• Temporary suspension of user access to HSC information assets.</li> <li>• Re-training and re-evaluation.</li> <li>• Discussion of policies and procedures.</li> <li>• Oral warning or reprimand.</li> <li>• Letter of Counseling, or Letter of Reprimand; ineligible for bonus, transfer, or promotion for minimum of six months.</li> </ul>

		acquiring malicious software.	
2	<ul style="list-style-type: none"> <li>• Intentional Violation without Malice: A violation of UF HSC information security policy.</li> <li>• Second occurrence of level 1 violation involving Restricted or Sensitive information.</li> </ul>	<ul style="list-style-type: none"> <li>• Sharing individual passwords.</li> <li>• Failing to report a probable security violation.</li> <li>• Inappropriate sharing of Restricted or Sensitive information.</li> <li>• Using another user's UserID.</li> <li>• Allowing another user to access information using your User ID.</li> <li>• Using peer-to-peer (P2P) software on the HSC network.</li> <li>• Improper disposal of information assets</li> <li>• Storing or downloading Restricted information to an unauthorized computer or removable media</li> </ul>	<ul style="list-style-type: none"> <li>• Temporary suspension of user access to HSC information assets.</li> <li>• Re-training and re-evaluation.</li> <li>• Discussion of policies and procedures.</li> <li>• Letter of Reprimand with written corrective action, acknowledgement of consequences of subsequent infractions being immediate termination; ineligible for bonus, transfer or promotion for minimum of six to twelve months.</li> <li>• Suspension without pay.</li> </ul>
3	<ul style="list-style-type: none"> <li>• Intentional Violation with Malice: A violation of UF HSC information security policy with the intent to do harm.</li> <li>• Second occurrence of level 2 violation involving Restricted or Sensitive information.</li> </ul>	<ul style="list-style-type: none"> <li>• Intention to destroy or destruction of information assets not otherwise scheduled for destruction.</li> <li>• Intentional inappropriate access or sharing of Restricted or Sensitive information.</li> </ul>	<ul style="list-style-type: none"> <li>• Termination of employment (Employee ineligible for re-hire or for future information access.</li> <li>• Recommend revocation of Medical Staff privileges in accordance with the by-laws.</li> <li>• Termination of user privileges.</li> </ul>