Standard: GP0003.04	Category: General Provisions	Version Date: 09/02/2009
Title: **Information Security Program Definitions**		Effective Date: 12/05/2008
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 provide a consistent set of definitions for terms used in the Information Security Program.

References:

1. The SANS (SysAdmin, Audit, Network, Security) Institute "Glossary of Terms Used in Security and Intrusion Detection": http://www.sans.org/resources/glossary.php
2. WikipediA Online Encyclopedia - Technology and Applied Sciences: http://www.wikipedia.org

Standard:

1. The referenced glossary of terms is the standard glossary for the UF HSC Information Security Program for those terms that appear in it unless the legal or UF HSC definition is different. If the legal or UF HSC definition is different, the legal or UF HSC term is defined in this standard and overrides the SANS definition. Terms used by the UF HSC and not listed in the SANS glossary are also defined in this standard.
2. Abuse of Privilege: A user willfully performing an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.
3. Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
4. Information system: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
5. Account: A username and password combination allowing authenticated access to the UF HSC Information and Computing Environment.
6. Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

7. Administrator Special Access Account: Any account with special and/or elevated access privileges. Technical support staff, security administrators, system administrators and others responsible for management and operational functions of an IT-Resource may be granted special access accounts.
8. Application Administration Account: Any Account intended for administration of an application (e.g., Oracle database administrator, MS-SQL administrator).
9. Attack: A specific formulation or execution of a plan to obtain unauthorized access to files and programs or the control state of a computer system. Success or the lack thereof has no bearing on this definition.
10. Authentication: The corroboration that a person or entity is the one claimed.
11. Availability: The property that data are or information is accessible and useable upon demand by an authorized person.
12. Backup: Copy of files and applications made to avoid loss of data and facilitate recovery of data and information.
13. Best Practices - A case study, technical analysis, and/or instructional information that provides a benchmark for practices in achieving a desired result. While not mandatory, best practice guidelines are intended to be informational, to facilitate knowledge transfer, and to shorten the learning curve for entities addressing common issues.
14. Compromised Host: A system to which an intruder has gained access in excess of that intended to be available.
15. Computer Incident Response Team: UF HSC and Unit personnel responsible for coordinating the response to computer security incidents in a Unit.
16. Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.
17. Countermeasure: A procedure, action, device, or anything else that has the ability to reduce the level of a vulnerability.
18. Crucial Asset: Information assets, and any other types of assets (e.g., emergency power sources or cooling systems) that are absolutely necessary to the function of the unit, or the loss or unavailability of which presents an unacceptable risk to the unit's business processes, data or data security.
19. Custodian: Individual or organization assisting an Owner with hosting or operating an Information Asset according to assigned responsibilities.
20. Delegate: Those persons to whom the designee has delegated authority to establish information classification/security requirements for selected sets of information.
21. Designee: Those designated by the President of the University as having specific authority which, for the purposes of the Security Program, includes establishing information classification/security requirements.
22. Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.
23. Electronic mail system: Any computer software application that allows electronic mail to be sent from one computing system to another.

24. Email: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.
25. Emergency Change: An unauthorized immediate response to imminent critical system incident needed to prevent widespread service disruption.
26. Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
27. Facility: The physical premises and the interior and exterior of a building(s).
28. Filter: A control used to block access to an IT resource which may or may not include a specific port.
29. Firewall: An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.
30. Guideline: A specific approach, solution, methodology, product, or protocol for establishing uniformity that should be followed when implementing policies unless justifiable reasons for a variance exist. May also serve as objectives for procedures.
31. HealthNet: The communications infrastructure management group for all UF HSC managed spaces, both at the UF campus facilities proper and to all UF HSC facilities off-site. Members of the UF HSC Community housed in space administered by other infrastructure management groups must meet the same minimum requirements, but are subject to additional provisions as outlined by that other infrastructure management group.
32. HSC: Health Science Center at the University of Florida including off-campus locations.
33. Information Asset: see UF HSC Information Asset.
34. Information Asset Disaster: An occurrence which results in the loss, destruction, theft or corruption of information assets, an inability to access information that cannot be resolved in a reasonable time period, or damages or compromises systems or processes which are necessary for the confidentiality, integrity and availability of information.
35. Information Attack: An attempt to bypass the physical or information security measures and controls protecting an Information Asset. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures. Success or the lack thereof has no bearing on this definition.
36. Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.
37. Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and universities.
38. Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an

organization. An organization's intranet may be protected from external access by a firewall and/or any other authentication technology.

39. Internet Protocol (IP) Address: A unique number/character combination assigned to computers, instruments, printers, machines, appliances, network infrastructure device for purposes of enabling communication between them and ensuring information is routed to its intended destination accurately and expediently. You typically see IP addresses in this format: 255.255.255.255.
40. IT Resource: Any equipment that has the primary purpose to store, process, display or transport digital information in support of the UF mission is a UF IT resource. The associated data, applications and hardware, are also IT resources.
41. Local Area Network (LAN): A data communications network spanning a limited geographical area. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.
42. Malicious Software: Software designed to damage or disrupt a system. Examples are: viruses, worms, Trojans, denial of service and other such attacks. Sometimes referred to as rogue programs.
43. Maskable IP range – A set of contiguous IP addresses that can be described in a DHCP configuration, firewall rule, router access control list and other technical configurations with just one sub network name. A common analogy is the use of a zip code in the flow of mail to a large number of street addresses. The use of maskable IP ranges reduces complexity (risk of mistakes) and improves configuration efficiency by eliminating the need to type or cut and paste many IP addresses into configuration files.
44. Networked Device: Any computer, instrument, printer, machine, appliance etc that is capable of accessing other computers, instruments, printers, machines, appliances or other devices as a result of its connection to a component on the HealthNet network infrastructure (switch, router, hub, bridge, access point, *etc.*)
45. Network Service Providers: Organization responsible for managing the network and keeping it operational for all network users. Computer Network Services (CNS) for the internet connection used by the HSC; HealthNet for the wired and wireless network installed in HSC facilities with the exception of any network areas designated as Shands wired or wireless network; Shands Information Services (IS) for the wired and wireless network installed in Shands Healthcare facilities with the exception of any network areas designated as HSC.
46. Offsite Storage: Based on information criticality, offsite storage should be in a geographically different location from an Information Asset. Based on an assessment of the data backed up, removing the backup media from the building and storage in another secured location in the UF HSC may be appropriate.
47. Owner: The University of Florida owns all information assets acquired through the University or its affiliates. All information assets generated, in the course of employment, by the faculty, staff, and other employees of the University and its affiliates are also owned by the University of Florida except as may be specified in a

contractual agreement with an employee.

48. Password: Confidential authentication information composed of a string of characters.
49. Personal information: as specified by the Florida Statutes means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:
    a. Social security number.
    b. Driver's license number or Florida Identification Card number.
    c. account number, credit card number, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

    Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
50. Personally or Affiliate Owned computer: computer purchased with non-UF funds such as a user's personal finances (*i.e.*, student), or another institution or company's funds (*i.e.*, a visiting colleague or vendor) and not with UF funds.
51. Phishing – see social engineering.
52. Physical Safeguards: Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
53. Policy: A mandated course of action or behavior that is followed. Policies are usually point-specific, covering a single area.
54. Portable Computing Devices: Any small lightweight portable device capable of receiving and/or transmitting data. These include, but are not limited to, notebook computers, handheld computers, Personal Digital Assistants (PDAs), pagers, and cell phones.
55. Practice: See Best Practices.
56. Primary Account Number (PAN) – A customer's full credit card number.
57. Procedure: A set of instructions for implementation of a policy using applicable standards.
58. Protected Health Information (PHI): individually identifiable health information (as defined by HIPAA privacy regulation):

    (1) Except as provided in paragraph (2) of this definition, that is:

        (i) Transmitted by electronic media;

        (ii) Maintained in electronic media; or

        (iii) Transmitted or maintained in any other form or medium.

    (2) Protected health information excludes individually identifiable health information in:

        (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
(iii) Employment records held by a covered entity in its role as employer.

59. Restricted Information: Data whose loss, corruption, or unauthorized disclosure would seriously and adversely impact the academic, business or research functions of UF HSC. The impacts on UF HSC could include any violation of privacy, business, financial, legal or UF HSC contracts, or a violation of federal or state laws/regulations. Examples include, but are not limited to, statutorily protected medical information, litigation documents, and UF HSC strategy documents.
60. Scheduled Change: Formal notification received, reviewed, and approved by means of a review process and appropriate authority in advance of a change.
61. Security or Security Measures: encompass all of the administrative, physical, and technical safeguards in an information system.
62. Security incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
63. Social Engineering: the practice of conning people into revealing sensitive data on a computer system, often on the Internet. A good reference is *The Art of Deception*, by Kevin Mitnik and William L. Simon.
64. Standard: A specific approach, solution, methodology, product, or protocol that must be adhered to for establishing uniformity when implementing policies. Standards may serve as objectives for procedures.
65. Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.
66. Subsidiary Unit: A major unit which has a distinct and divergent mission statement from that of UF, and which in some cases may also be a separate legal entity, such as Shands.
67. System Administrator: Person responsible for the effective operation and maintenance of an IT Information Asset, including implementation of standard procedures and controls, to enforce an organization's security policy.
68. Technical safeguards: The technology and technical policy and procedures for the application of technology that protect information assets and control access to them.
69. UF HSC Information and Computing Environment: The combination of Information Assets owned, leased, administered, maintained, operated or otherwise under the custody or control of the Health Science Center at the University of Florida.
70. UF HSC Information Asset:
    a. Information that is owned, managed, and/or used by UF HSC in any form (electronic, paper, film, *etc.*);

b. The asset used to create or house information (workstation, film library, file cabinet, *etc.*);
c. The terms "information" and "data" are used interchangeably in the context of the Information Security Program.

71. UF Information Security Manager (ISM): The person identified by the University of Florida responsible for coordinating security efforts including, but not limited to, risk assessment, enterprise network intrusion detection, maintaining Unit ISM contact information, working with Unit ISMs to resolve exposures and reduce potential exposures, monitoring the UF security web site, and organizing IT security training events.
72. UF Managed devices – devices that are managed under the supervision of an HSC authorized and documented Unit ISM. Such devices generally include department issued and supported workstations, servers and printers. ISMs recognized by UF main campus are authorized but need to be documented on the HSC ISM list.
73. UF Owned computer: computer purchased with any funds associated with the UF including departmental, HSC, grant, contract, education, FCPA, special *etc.*, computer donated to the UF, or computer acquired through a service funded by the UF. Includes vendor managed computers purchased by any funds affiliated with the UF, and installed in a HSC facility.
74. Unit: A College, Department, Institute, or other administrative or logical subdivision/customer base in UF HSC.
75. Unit Information Security Manager (ISM): The person identified by the Unit responsible for coordinating information technology security efforts within that Unit.
76. Unit Information Security Administrator: The person identified by the Unit responsible for coordinating information security efforts within that Unit.
77. Unmanaged devices: UF or personally owned computers that are not managed under the supervision of an HSC authorized and documented Unit ISM. Such devices may pose more risk to the HSC because their security countermeasures are not under the direct control of the Unit ISM. Examples include vendor provided and supported devices, lab computers and servers supported by lab staff, personally purchased computers used for work, student computers.
78. Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerabilities.
79. User: A person or entity with authorized access.
80. Vendor: An individual or organization not part of UF HSC Community who supplies or manages an Information Asset.
81. Voice Contact: The designated Unit person responsible for all voice communication to/from the Unit.
82. Web Application: In software engineering, a web application or webapp is an application that is accessed via web browser over a network such as the Internet or

an intranet. Application software should be contrasted with system software which is involved in integrating a computer's various capabilities, but typically does not directly apply them in the performance of tasks that benefit the user. Application software sits on top of system software because it is unable to run without the operating system and system utilities. Web application software can be differentiated from other web presence software in that it will accept data input from a user and will interact with a database. Some web applications may not interact with a database, but will perform moderately complex logic or computations with the user input, and display the results for the user (e.g. mortgage calculation). In contrast a web page will interact with the user by displaying information or accepting and responding to navigation responses. The delineation between web page code and web application code is not always evident; where programming code is applied, secure programming practices should be addressed.

83. Web page: A document on the World Wide Web. A unique URL (Uniform Resource Locator) identifies every Web page.
84. Web site: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.
85. Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.