UF UNIVERSITY of FLORIDA
Information Technology

Standard

Standard: GP0005.02	Category: General Provisions	Version Date: 2/1/2017
Title: **Security Education and Awareness Standard**		Effective Date: 2/15/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/1/2017
Reviewer: HIPAA Security Officer		Next Review: 2/1/2020

Purpose:

To establish topics for inclusion in training system users to comply with Policy TS0002.

Reference(s):

1. Policy GP0005: Security Education and Awareness Policy.
2. The University of Florida Information Technology Policies: http://www.it.ufl.edu/policies/
3. UF Acceptable Use Policy: http://www.it.ufl.edu/policies/acceptable-use/acceptable-use-policy/
4. UF Information Security Training information and links: https://security.ufl.edu/learn-information-security/

Standard:

Information Security general awareness education and materials are expected to be provided to all members of the UF workforce. The topics should be selected and adapted based upon the users' role. Additional topics may be addressed at the discretion of the Unit.

1. Identify who the Unit Information Security Administrator (ISA) and Unit Information Security Manager (ISM) are for that user.
2. Make sure the user understands that they must comply with all UF/HSC policy and standards, including, but not limited to:
    a. Software Copyright policy;
    b. UF Acceptable Use Policy;
    c. UF Information Security
3. Describe how your unit handles electronic communications, including, but not limited to:
    a. Facsimiles;
    b. E-mail;
    c. Instant Messaging;
    d. Voice;
    e. Audio;
    f. Video Conferencing.
4. Basic computer information to include:

   a. Malicious Software (*Malware*) Protection Controls – what this is and how often the updates and scans are to be done to protect against viruses, spyware and adware.
      i. E-mail Attachments – if you weren't expecting an attachment, exercise caution when opening the attachment. If possible, make sure your anti-virus software scans incoming email.
      ii. You've received an email (that may be offensive) yet you do not know the person who sent the email – This is likely the result of an email worm or Trojan that has mined a list of email addresses and found yours.
      iii. Each unit should explain how suspected malware e-mail should be handled.
      iv. Explain Social Engineering and what to do about it.
   b. Software updates and patches
      i. Why do them;
      ii. Who does them;
      iii. How often this should be done.
5. Describe how your unit handles network/application access.
6. Basic password management information such as:
   a. Keep it secure;
   b. Don't use someone else's;
   c. Change often;
   d. If a user thinks someone has learned their password – they should involve the Unit ISM for guidance on what to do.
7. Describe how your unit handles encryption for:
   a. Electronic communications.
   b. Electronic storage.
8. Describe how your unit handles data storage on the computer and on removable media (diskette, cd, dvd, tapes, *etc.*), including:
   a. When not in use, secure all media that is received or created.
   b. Consult Unit ISM on how to properly destroy and/or reuse computers, portable computing devices and electronic media once it is obsolete.
   c. Use of encryption.
9. Basic Portable Computing Device (PCD) information such as:
   a. Keep them secure when not in use.
   b. Have reasonable safeguards in place (password or encryption).
   c. Shall not be used to store long term restricted information.
10. General File Downloads and Installations, including:
   a. Be mindful of what is downloaded and from what sites. Downloading and running unknown programs may open a system to attack. All downloaded files should be scanned with a current anti-virus program using current virus definition files.
11. Basic Physical Security information to include:

a. Make sure offices are kept secure;
b. Explain how visitors should be handled;
c. Explain how computing assets should be kept physically secure;

12. Describe what protected health information, personally identifiable information, and student records are and that they are legally protected.
13. Explain how observed security, policy or standard violations must be reported to the Unit ISA , the Unit ISM, Privacy Office and/or the Supervisor.
14. Explain how department file shares may and may not be used to store Restricted information.
15. Explain that Peer2Peer (P2P) applications may not be used in the HSC information and computing environment.