UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

POLICY

Policy: TS0011	Category: Technical Security	Version: 2/15/2008
Title: Software Security Compliance		Effective Date: 04/01/2008
Originating Unit: Security Program for the Information and Computir Environment Project		Last Review: 02/15/2008
Review Resp: HSC Chief, Information Security		Next Review: 02/2010

Purpose:

To ensure that software installed on UF HSC Computing Devices contains adequate security features to prevent unauthorized access, use, modification or destruction of information.

Scope:

This policy applies to all software installed in the UF HSC computing environment or intended to be used to create, store or maintain UF HSC information.

References:

1. University of Florida Software Copyright Policy issued by the Office of Information Technology. http://www.it.ufl.edu/resources/copyright/POLICY.HTM.
2. UF Guidelines to Develop Applications for Secure Deployment. http://www.it.ufl.edu/policies/guidelines.html
3. University of Florida Finance and Accounting Directive 1.4.11.12 Credit Cards, E-Commerce Security and Management Policy: http://fa.ufl.edu/uco/handbook/handbook.asp?doc=1.4.11.12
4. Payment Card Industry Data Security Standards: https://www.pcisecuritystandards.org/
5. SPICE Standards:
    a. TS0011.01General Software Security
    b. TS0011.05 Web Application Security
    c. TS0011.10 E-Commerce Applications and Card Holder Data Security
6. SPICE Evaluation Program
    a. Products and Services Security Evaluation Procedures
    b. EV0001 – Information Technology Products and Services Security Evaluation Form

    https://security.health.ufl.edu/isa_ism/eval_artifacts.shtml

Policy:

1. When applicable, software must be compliant with the above referenced policies, directives and standards.

2. The Unit ISM must ensure an up-to-date inventory of software owned or used by the Unit for the creation, maintenance or storage of Restricted or Sensitive Information ("Software Inventory") is maintained. An inventory of software not handling Sensitive or Restricted information should be maintained current.
3. Individuals who install, develop, upgrade, or modify software on a HSC Information Technology (IT) Resource, including end user workstations, are responsible for notifying the Unit Information Security Manager (ISM) about the software for purposes of inventory and security evaluation.
4. The use of non-University purpose software, such as software for personal, entertainment or non-University business use is subject to departmental policy. When permitted, such software must also comply with this policy.
5. The Unit must perform a security evaluation on new software purchases, development, major upgrades, enhancements, platform migrations, application service provider (ASP) and software as a service (SaaS) solutions.
    a. The software security evaluation process used must be one that is approved by the HSC Security Office (see SPICE Security Evaluation Program in references.)
    b. The recommendations generated from the security evaluation must be completed prior to use of the software on production systems, prior to use by users and prior to interaction with Restricted or Sensitive information unless otherwise stated in the evaluation report.
    c. The UF HSC Security Office may require or initiate security validation testing for the purpose of identifying vulnerabilities.
    d. Software determined by the security evaluation process to present an unacceptable security risk to the HSC is prohibited from accessing or using the HSC network, and from interacting with HSC Restricted or Sensitive information.
6. The Unit ISM and/or the Unit ISA in concurrence with the HSC Security Office may at any time require an individual to uninstall or remove software that has been verified to create an unacceptable security risk.
7. Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the software and the individual violating the policy.