UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: TS0011.01	Category: Technical Security	Version Date: 2/15/2008
Title: General Software Security		Effective Date: 4/1/2008
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 2/15/2008
Review Resp: HSC Chief, Information Security		Next Review: 2/2010

Purpose:

To provide a source of recommended security controls for computer software used in the HSC computing environment.

References:

1. SPICE Policy TS0011 Software Security Compliance.
2. UF Guidelines to Develop Applications for Secure Deployment. http://www.it.ufl.edu/policies/guidelines.html
3. 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

Standards for All Software:

1. Software Inventory - Unit software inventories shall at a minimum indicate the following information:
    a. Name of the software
    b. Purpose
    c. Business Owner (Administrative contact whose operation depends on the software)
    d. Technical Ownership
        i. Current UF HSC Technical contact
        ii. Vendor/contractor (if applicable)
    e. Classification of the information that it creates, captures, stores or processes:
        i. Restricted and what type:
            1. Protected Health Information (PHI)
            2. Social Security Numbers
            3. Student Records
            4. Credit Card Numbers
            5. Other
        ii. Sensitive
        iii. Operational
        iv. Unrestricted

f. Authorization Status (optional)
    i. Authorized for use
    ii. Authorized exception
    iii. Not Authorized
g. Recoverability objectives (after loss of system availability, the period of time that an operation can rely on a contingency operation without detrimental effects to the customers the operation serves) in terms of:
    i. Recovery time objective:
        1. 0-24 hours
        2. 0-72 hours
        3. 0-120 hours
        4. As resources are available
    ii. If applicable, recovery point objective (latency of data that can be tolerated)
h. Location
    i. If server based, unique machine name or DNS name of the server, its system administrator, and the data center location
    ii. If client based, estimate of the number of clients and buildings where the client software is installed
i. External system dependencies – other systems not in control of the Unit that the software depends upon to operate correctly (i.e. Gatorlink Authentication, critical data feeds, etc.) and a technical support contact name for the external system.

2. General security features *that must be examined in all* acquired or developed software products while evaluating and testing other features, and prior to actual use on production systems or by users, are as follows:
    a. Compatibility with Security Standards
        i. Does not require the use of unauthorized mechanisms for remote access to the software, such as
            1. Unencrypted transmission
            2. Undocumented ports
            3. Unauthorized or undocumented access accounts
        ii. Will not disable or circumvent standard antivirus protections, authentication, automated OS patch management or other security controls on the end user device, server or network.
        iii. Does not require elevated system rights in the OS to run.
    b. If third party software, it has been acquired through a credible source:
        i. The software should be in use in other locations; reviews should be available and should be researched.
        ii. The software should be acquired from a known credible software source that has a history and reputation for distributing trouble free and legally acquired software.
    c. Technical support and maintenance are clearly identified and provisioned to maintain the software throughout the life of the software.

i. Version maintenance responsibility is clearly defined to ensure software continues to comply with these standards and remains compatible with an OS that is still vendor supported with security patches.

Standards for Software that Handles Restricted or Sensitive Information:

3. General security features that *must be evaluated and documented* in all acquired or developed software products *prior to testing or use in capturing, storing, processing or transmitting Restricted or Sensitive information*:
    a. User, device and process authentication
        i. Requirement to authenticate
        ii. Capability to use Gatorlink authentication credentials
        iii. Capability to integrate with UF AD, LDAP or Kerberos systems
        iv. Password management
            1. Configurable password strength
            2. Configurable password expiration
            3. Password protection (encryption, non-display field)
            4. Configurable password inactivity deactivation
        v. Protection from password brute force (automated or robotic) attack
    b. Authorization
        i. Applies least privileged principle to the application's access to the host computer it is running on and the database it accesses.
        ii. Role based authorization
            1. Pre-defined roles
            2. Capability to customize roles
        iii. Variability of grantable role privileges
            1. Function (view, add, modify, delete, approve, query, etc.)
            2. Record/Data (limit access by attribute of a patient or student)
            3. Account/Security management is separate from other functions
    c. Activity logging
        i. Function (what user has done to a record)
        ii. Record/Data (what record user has accessed)
        iii. Easy to read audit reports or reporting capability (example)
        iv. Log data management functions
            1. logs can be sent to a central database
            2. logs can be put on an automated archival schedule
            3. logs can be put on an automated purge schedule
        v. What is logged is configurable
        vi. Access to activity logs and audit reports can be restricted

vii. Access to activity logs is logged

d. Data security
   i. Data stored by the software on end user devices without user intervention, knowledge, or opportunity to prevent are encrypted or otherwise protected.
   ii. Easily integrates with standard encryption solutions such as SSH, SSL, TLS & VPN.

e. Data Integrity
   i. Pulldown selection boxes wherever possible to control user input
   ii. Validity checking on all free form user input fields
   iii. Checksum, hashing or other integrity control mechanisms to ensure integrity of data through an interface

f. User Security Awareness and Responsibility Materials
   i. Availability of acceptable use standards or guidelines specific to the software and the data to which it provides access
   ii. Appropriate security warnings on high risk user controlled software features, such as data exports and downloads.
   iii. Informing user of activity logging (consider making activity records of end user available to him/her)

4. The security features listed above are elaborated in the SPICE products and services security evaluation process and procedures which should be performed prior to resource investment (i.e. buying a product, expending integration effort, or writing code) in new software or software services. The procedures and evaluation form are in the references above.
5. 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.