PROCEDURE

Subject:	**Software Development and System Integrations**	**Number:** 2.60.08
Source:	Vice President, Planning and Institutional Effectiveness	**Reference (Rule #)** 6HX14-2.60
President's Approval/Date:	**4/10/18**	

PURPOSE:

This procedure outlines how to manage the software development and systems integrations processes to assist State College of Florida (SCF) and its service providers to comply with state law, federal law, SCF procedures and rules, as well as the security frameworks.

SCOPE:

This procedure applies to:

- Users, systems, and locations;
- Employees, contractors, service providers; and
- Applies to all facilities.

This procedure applies to any software or integrations being developed or acquired that process confidential or restricted information (as defined in the SCF Data Classification Guidelines).

POLICY STATEMENT:

Security Requirements Identification Prior to Development/Acquisition

Before a new system or integration is developed or acquired, SCF must have clearly specified the relevant security requirements. Alternatives maybe reviewed with the developers and/or vendors, so that an appropriate balance is struck between security and other objectives (ease-of-use, operational simplicity, ability to upgrade, acceptable cost, etc.). Systems designers and developers must consider security from the beginning of the systems' design process through conversion to a production system.

Formal Specifications Required for Software Development/Acquisition

All software and integrations developed by in-house staff or acquired should have a written formal specification. This specification must be part of an agreement between the involved information owner(s) and the system developer(s). A first draft of the agreement must be completed and approved prior to the time when programming or acquisition efforts begin.

Systems Designers and Developers Must Report Problems

All potentially serious problems associated with information systems or integrations being designed or developed, which are not being adequately addressed by planned or existing projects, must be promptly reported to the Information Security Team (ITSecurity@scf.edu).

Removal of All Unauthorized Access Paths in Production Software

Prior to moving software which has been developed in-house to production status, programmers and other technical staff must remove all special access paths, so that access may only be obtained via normal secured channels. This means that all trap doors and other short cuts that could be used to compromise security must be removed. Likewise, all system privileges needed for development efforts, but not required for normal production activities, must be removed.

Naming Convention for Production Files

Transactions used for auditing, testing, training or other non-production purposes must be labeled and/or otherwise separated from transactions used for production processing. This will help ensure that SCF records are not improperly updated by non-production transactions.

File Naming Convention

A file naming convention must be used to clearly distinguish between those files used for production purposes and those files used for testing and/or training purposes.

Systems Utilities Resident on Production Systems

Disks and other on-line storage facilities used on production systems must not contain compilers, assemblers, text editors, word processors or other general purpose utilities which may be used to compromise the security of the system.

Separation Between Development, Testing and Production Environments

Business application software in development, testing and production must be kept strictly separate. If existing facilities permit it, this separation must be achieved via physically separate computer systems. When computing facilities do not allow this, separate directories or libraries with strictly enforced access controls must be employed.

NONCOMPLIANCE: Any employee/contractor found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Service providers found to have violated this procedure may be subject to financial penalties, legal action, and including termination of contract.