

Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

System Development Policy: IT-08

Introduction:

In order to be successful, all major application projects must undergo a well-defined development lifecycle. This policy establishes the minimum requirements and responsibilities for SHSU lifecycle development.

Software development is a complex endeavor, susceptible to failure, unless undertaken with a deliberate and systematic methodology. Software Development Lifecycle (SDLC) is a methodology for implementing an application project by following a sequence of standard steps and techniques. In combination with sound project management, the SDLC improves the capability of application projects to deliver as expected, on time, and within budget. Besides increasing the success rate of application projects, the SDLC also facilitates TSUS and statewide collaboration in application projects. Finally, SDLC increases the efficiency and effectiveness of SHSU's software development personnel.

Scope:

The SHSU System Development policy applies equally to all individuals installing or developing software applications.

Policy Statement:

1. IT@SAM is responsible for developing, maintaining, and participating in a SDLC for SHSU system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. To ensure that the software will be adequately documented and tested before it is used for critical applications at SHSU, this plan should address at a minimum the following areas:
 - a. Stakeholder identification and involvement;
 - b. Preliminary analysis or feasibility study;
 - c. Risk identification and mitigation;
 - d. Systems analysis;
 - e. General and detailed design;
 - f. Development or acquisition;
 - g. Quality assurance and acceptance testing;
 - h. Implementation; and
 - i. Post-implementation maintenance and review.
 - j. This methodology ensures that the software will be adequately documented and tested before it is used for critical information. Additionally, this methodology ensures that projects match the strategic direction of the university and compliance with guidelines.
2. All production systems must have designated Data Owners and/or Data Custodians who manage the user access control system restricting who can

- access the system as well as restricting the privileges available to these users.
3. IT@SAM must perform periodic risk assessments of production systems to determine whether the controls employed are compliant.
 4. Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems unless authorized for quality assurance. Likewise, all production software testing must utilize sanitized information.

Related Policies, References and Attachments:

An index of approved IT@SAM policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2014