

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.25</b>	<b>Systems Development Life Cycle (SDLC) Policy</b>	Responsibility:	Chief Information Security Officer

# SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC) POLICY

---

## Overview

This document addresses Systems Development Life Cycle (SDLC) processes at the Health Science Center, including UT Medicine. A structured process for software development is needed to ensure critical systems or systems that require moderate to significant development resources are developed to meet management's goals in a secure and efficient manner. The SDLC process must address requirements definition, design, development, quality assurance and acceptance testing, implementation, change management, and post-implementation maintenance.

There are several different models that can be utilized as a framework to develop sound SDLC processes. DIR's Texas Project Delivery Framework includes an SDLC extension that is based on the V-model at [DIR SDLC Extension](#) that can be used to help develop local SDLC procedures. The [DIR SDLC Extension](#) also contains appendices that describe other models such as:

- Incremental System Development Life Cycle
- Rapid Application Development
- Agile

---

## Policy

1. To ensure reliable and stable systems, all departments developing software applications are required to establish best practice SDLC procedures and require compliance from individuals who develop new systems.
2. This policy does not apply to research (scientific discovery) projects funded or otherwise.
3. All systems development requires prior approval by the appropriate Dean, Director, Chair, or designee.
4. All systems developed in-house, must be documented through a SDLC process. Based on risk, each department should

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.25</b>	<b>Systems Development Life Cycle (SDLC) Policy</b>	Responsibility:	Chief Information Security Officer

---

develop/formalize development procedures considering the following:

- Preliminary analysis or feasibility study
  - Risk identification and mitigation
  - System analysis
  - General design and detail design
  - Development
  - Quality assurance and acceptance testing
  - Implementation
  - Post-implementation maintenance and review
  - Issues management
5. SDLC controls must also be in place for departments that purchase computer applications and/or contract with Application Service Providers (ASP) for an outsourced application solution.
6. Based on risk, outsourced solutions must be properly secured and backed-up. Contracts must address security, back-up, disaster recovery, privacy requirements, and ensure compliance with applicable laws, rules, and regulations. Finally, contracts should include right-to-audit provision to provide appropriate assurances that contractual obligations are met.

---

### **Definitions**

**MODERATE TO SIGNIFICANT DEVELOPMENT RESOURCES:** The following is provided as guidance for a risk based approach to determining whether a formal SDLC procedure should be in place. Note that projects which satisfy two or more of the following criteria typically should have a formal SDLC procedure.

- Out-of-pocket 3 year implementation and recurring costs exceed \$100,000

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.25</b>	<b>Systems Development Life Cycle (SDLC) Policy</b>	Responsibility:	Chief Information Security Officer

- 
- Implementation hours exceed 1,000 hours
  - Impacts broad numbers of users throughout the Health Science Center
  - Satisfies Health Science Center strategic goals
  - Requires interoperability with existing IT systems/data
-