Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	June 2018
Policy 5.8.25	**Systems Development Life Cycle (SDLC) Policy**	Responsibility:	Chief Information Security Officer

SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC) POLICY

Overview

UT Health San Antonio shall adopt policies, standards and procedures to ensure the protection of Information Resources (including data confidentiality, integrity and availability) is considered during the development or purchase of new Information Systems or services.

Policy

The Chief Information Security Officer (CISO) shall develop policies, standards and/or procedures that address the following:

1. Providing methods for appropriately restricting privileges of authorized Users to all production systems, applications, data and University-owned devices. User access to applications is granted on a need-to-access basis;

2. Maintaining separate production and development environments to ensure the security and reliability of the production system;

3. Performing a security assessment prior to the purchase of any new information security services that receive, maintain, and/or share Confidential Data;

4. Performing vulnerability assessments and code scans on a periodic basis and based on risk of the data and/or Information Resource; and

5. Performing vulnerability assessments and including a static or dynamic code scan of all new or significantly upgraded/changed Web applications prior to moving them to production.

The Chief Information Security Officer must review and approve security requirements, specifications and, if applicable, third-party risk assessments for any new computer hardware, software, applications or services that are Mission Critical or that receive, maintain, and/or share Confidential Data.

- Contracts for purchase or development of software applications must address security, backup and privacy requirements and should include right-to-audit and other provisions to provide

appropriate assurances that applications and data will be adequately protected.

Information Systems that duplicate services (e.g., electronic mail, web and file services) provided by Information Management and Services (IMS or Centralized IT) are prohibited unless approved by the Vice President and Chief Information Officer.

- The Owner of the duplicated Information System must document and justify exceptions based on business need, weighed against risk of unauthorized access or loss of data.

Software Development

To ensure reliable and stable systems, all departments developing software applications are required to establish best practice Software Development Life Cycle (SDLC) procedures and require compliance from individuals who develop new systems.

1. This policy does not apply to research (scientific discovery) projects funded or otherwise.

2. All systems development requires prior approval by the appropriate Dean, Director, Chair, or designee.

3. All systems developed in-house, must be documented through a SDLC process. Based on risk, each department should 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

4. SDLC controls must be in place for departments that purchase computer applications and/or contract with Application Service Providers (ASP) for an outsourced application solution.

Online and Mobile Applications

Before deploying an Internet website or mobile application that processes confidential information, the developer or Information Resource Owner of the website or application must:

1. Submit to the Chief Information Security Officer information describing:
   - the architecture of the website or application;
   - the authentication mechanism for the website or application; and
   - the administrator level access to data included in the website or application.
2. Subject the website or application to vulnerability and penetration tests conducted internally by the CISO and in compliance with all UT Health policies, standards and procedures.
3. Mitigate all classified “high” and “critical” vulnerabilities and risks identified through vulnerability and penetration testing.

Reference

- U.T. System Policy 165 Standard 21