5.8.25 System Development and Deployment

Chapter 5 - Information Technology	Original Effective Date: October 2004
Section: 5.8 Information Security	Date Last Reviewed: July 2022
Responsible Entity: Chief Information Security Officer	Date Last Revised: July 2022

I. Purpose

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.

II. Scope

This policy applies to the development and deployment of information systems or services.

III. Policy

A. 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 solution that receive, maintain, and/or share confidential data.
4. Performing vulnerability assessments and code security scans as part of the Information Systems development cycle; 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.

B. The CISO 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.

C. 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 protected.

   Information systems that duplicate services (e.g., business systems, electronic mail, web, and file services) provided by UT Health San Antonio Information Technology (UTHSA-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.

D. Software Development

   1. To ensure reliable and stable systems, all departments developing software applications are required to establish information security and privacy considerations, security testing and audit controls in all phases of the system development lifecycle (SDLC).
      a. The information systems owner (owner) defines and documents information security and privacy roles and responsibilities throughout the SDLC.
      b. Identifies individuals having information security and privacy roles; and
      c. Integrates university information security and privacy risk management processes into SDLC activities.
   2. This policy does not apply to research (scientific discovery) projects.
   3. All systems development requires prior approval by the appropriate dean, director, chair, or designee.

E. Online and Mobile Applications

   Before deploying an Internet website or application or mobile application that processes confidential information, nonpublished research data or other sensitive classified intellectual property, the information resource owner must:

   1. Submit to the CISO information describing:
      a. the dataflow and system design architecture.
      b. the authentication mechanism.
      c. the audit controls; and
      d. 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 prior to deployment.

IV. Definitions

There are no defined terms used in this policy.

V. Related References

The University of Texas System, UTS Policy 165, Standard 21.

Texas Administration Code 202 Security Control Standards Catalog, SA-3 System Development Life Cycle.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

C.

Effective Date	Action Taken	Approved By	Date Approved
10/2004	Policy Origination		
06/2018	Policy Revision		
07/2022	Policy Revision, discretionary edits	CISO/ICPO	07/22/22