THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: SC-003.02-Application System Security Features	
Version 7	**Effective Date: 03/20/2016**

Responsible Office: Office of Cybersecurity	Last Review: 02/14/2023 Next Review: 02/14/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To require that Application Systems installed in UTHSC meet specified security features to prevent unauthorized use, access, transmission, modification, or destruction of UTHSC data or information. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

All Application Systems installed and/or used in UTHSC that process, store, access or transmit UTHSC data or information.

Definitions

Application - the system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.

OWASP – Open Web Application Security Project - an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. The Open Web Application Security Project provides free and open resources.

Responsibilities

UTHSC developers are responsible for ensuring that any custom-developed Application Systems developed and deployed by UTHSC must meet security features listed in this Practice.

Practice

1. All Application Systems shall be included in an Application System Inventory and at a minimum indicate the following information:
   a. Name of the Application System
   b. Purpose of the Application System
   c. Data or Information Owner
   d. Application System Custodian
   e. Vendor/contractor (if applicable)
   f. Classification of the data that it creates, captures, stores or processes referenced in GP-002-Data & System Classification
   g. Type of Information:
      - Protected Health Information (PHI)
      - Personal Identifiable Information (PII)
      - Student Records and other related FERPA data
      - Credit Card Numbers
      - Other
   h. Recoverability objectives (after loss of system availability, the period of time that an operation can rely on a contingency operation without detrimental effects to the customers the operation serves) in terms of:
   i. Recovery time objective:
      - 0-24 hours
      - 0-72 hours
      - 0-120 hours
      - As resources are available
   j. If server based, unique machine name or DNS name of the server and location.
   k. If client based, estimate of the number of clients and buildings where the client software is installed.
   l. External system dependencies – other systems not in control of the Unit that the software depends upon to operate correctly (i.e. Authentication systems, critical data feeds, etc.) and a technical support contact name for the external system.
2. Features for acquired or custom-developed Application Systems that must be examined in all acquired or developed software products while evaluating and testing other features, and prior to actual use in production or by users, are as follows:
   a. Compatibility with Industry Security Standards
   b. Does not require the use of unauthorized mechanisms for remote access to

the software, such as:
- Unencrypted transmission
- Undocumented ports
- Unauthorized or undocumented access accounts

c. Does not disable or circumvent standard antivirus protections, authentication, automated OS patch management or other security controls on the end user device, server, or network.
d. Does not require elevated system rights in the OS to run.
e. Third party software must be acquired through a credible and known credible software source that has a history and reputation for distributing trouble free and legally acquired software.
f. Technical support and maintenance are clearly identified and provisioned to maintain the software throughout the life of the software.
g. Version maintenance responsibility is clearly defined to ensure software continues to comply with security standards and remains compatible with an OS that is still vendor supported with security patches.
h. Users, devices, and processes are required to authenticate.
i. Authorization is based on the least privileged principle and Role based.
j. Users, devices, and process activity are logged per AU-002-Logging and System Activity Review.
k. Data stored by the software on end-user devices without user intervention, knowledge, or opportunity to prevent are encrypted or otherwise protected.
l. Documented evaluation and testing for Application System components and security features.

3. Security features that are for Web-based Application Systems must adhere to:
   a. The following Principles (see OWASP Principles for definitions):
      - Apply defense in depth (complete mediation)
      - Use a positive security model (fail safe defaults) (minimize attack surface)
      - Fail safe
      - Run with least system privilege
      - Avoid security by obscurity (open design)
      - Keep security as simple as possible to meet required security
      - Detect intrusions (compromise recording)
      - Does not trust infrastructure or external services
      - Established secure defaults
   b. Countermeasures (see OWASP Principles for definitions):
      - Access Control

- Authentication
- Canonicalization
- Cryptography and encryption
- Encoding
- Error Handling
- Input Validation
- Logging
- Mechanism
- Quotas
- Session Management
- Validation

c. Documented testing and results for Principles and Countermeasures listed above

4. A security evaluation should be performed prior to resource investment (i.e. buying a product, expending integration effort, or writing code) in new software or software services.
5. The recommendations generated from the security evaluation must be completed prior to use of the Application System in production, prior to use by users and prior to interaction with UTHSC data or information with a classification rating of 3 in any area unless otherwise stated in the security evaluation report.

References

1. SC-003-Application System Security
2. AU-002-Logging and System Activity Review
3. GP-002-Data & System Classification
4. Open Web Application Security Project