THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-003-Application System Security	
Version 6	**Effective Date: 03/20/2016**

Responsible Office: Office of Cybersecurity	Last Review: 04/15/2020 Next Review: 04/15/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

Software applications and systems are used at UTHSC to meet a variety of needs. This standard requires that as part of these information system's lifecycle, security features are considered an integral part of the planning, creating, testing, and deploying of information systems 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 Information Systems planned, created, tested, and installed at UTHSC that process, store, access or transmit UTHSC data or information. Information systems may be hardware only, software only, or a combination of both. The concepts and principles of this Standard apply to information systems that are either software only, or a combination of hardware and software (Application Systems).

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.

Responsibilities

Individuals who install, develop, upgrade, test, or modify Application Systems on UTHSC IT Resources, including end user workstations, are responsible for notifying the UTHSC Office of Cybersecurity about the Application Systems for purposes of inventory and security evaluation.

Said individuals are responsible for actively participating in the security evaluation

of the Information Systems.
UTHSC developers are responsible for ensuring that any custom-developed Application Systems developed and deployed by UTHSC must meet security features per SC-003.02-Application System Security Features to prevent unauthorized use, access, transmission, modification, or destruction of UTHSC data or information.

Standard

1. An up-to-date inventory of Application Systems installed, owned, or used for UTHSC must be maintained and kept current per SC-003.02-Application System Security Features, for any Application Systems used to access, transmit, modify, or store UTHSC data or information.
2. The use of Application Systems for non-UTHSC purposes, such as for personal, entertainment or non-UTHSC business use is subject to departmental policy. When permitted, such Information Systems must also comply with this standard.
3. A security evaluation on new Application Systems purchases, development, major upgrades, enhancements, platform migrations, application service provider and software, as a service solution, must be performed prior to use of the Application Systems in a production environment, prior to use by users, and prior to interaction with UTHSC data or information with a classification ranking of 3 in any area.
4. Application Systems determined by the security evaluation process to present an unacceptable security risk to UTHSC are prohibited from accessing or using the UTHSC network, and from interacting with UTHSC data or information with a classification ranking of 3 in any area.
5. UTHSC IT Security Team may at any time require an individual to uninstall or remove Application Systems that have been verified to create an unacceptable security risk.
6. Any custom-developed Application Systems developed and deployed by UTHSC must meet security features per SC-003.02-Application System Security Features to prevent unauthorized use, access, transmission, modification, or destruction of UTHSC data or information.
7. Any UTHSC Application System for credit card processing activities, including debit card processing and e-commerce activities must comply with FI0311 - Credit Card Processing.

8. Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the software and/or disciplinary action per GP-001.04-Information Security Violations for the individual(s) violating the policy.

References

1. GP-002-Data & System Classification
2. SC-003.02-Application System Security Features
3. GP-001-UTHSC Information Security Program
4. FI0311 - Credit Card Processing
5. GP-001.04-Information Security Violations