Texas A&M Health Science Center Guidelines

29.01.03.Z1.03 Guideline: Application Security

Approved February 13, 2013

Supplements System Regulation 29.01 and TAMU SAP 29.01.03.M1.21

Reason for the Guidelines

The Texas A&M Health Science Center (HSC) Application Security guideline establishes processes and coding practices to ensure development, deployment, and maintenance of secure applications. Adherence to the guideline will increase the security of applications and help safeguard confidential data and information technology resources.

1. Official Guideline

1.1. Application development tools and services should always connect using encrypted protocols whenever confidential or critical source code is transferred during connections. For example, connecting to source control systems or bug/ticket tracking systems should always be encrypted.

1.2. Application connections to external services like Lightweight Directory Access Protocol (LDAP) should use encryption.

1.3. Connections to database servers should be encrypted when possible or proper Access Control Lists (ACL) implemented.

1.4. When possible, all system and database passwords stored on configuration or scripts should be encrypted. Application libraries should read the encrypted passwords and decrypt them at runtime. This will ensure that if source code is compromised no critical passwords are stolen.

1.5. All database Structured Query Language (SQL) calls should use bind variables.

1.6. The use of standardized library repository systems that allow for a security audit of installed libraries is preferred, for example, Apache Maven or Ivy.

1.7. Applications requiring transmission of personal or private data should use Secure Sockets Layer (SSL) encryption.

1.8. HSC developed applications will always require server side validation and optionally client side validation. All errors should be logged.
1.9. Application logs are only required for debugging and troubleshooting problems or when they include audit information.

1.10. HSC developed applications require the web template, as outlined by the lead webmaster. Web templates will include links to HSC guidelines.

DISCIPLINARY ACTIONS

Violations of this policy may result in disciplinary action, which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution.

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration