1. GENERAL

The purpose of this Procedure is to describe the requirements for implementing application software that has been developed or acquired by authorized University personnel.

2. APPLICABILITY

This University Procedure applies to University information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this University procedure is to provide a set of measures that will mitigate information security risks associated with application development and acquisition. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience is University owners and custodians that manage applications that store or process Sensitive Information.

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions. The following definitions are for this document only.

Application means a configured piece of software, acquired or developed in-house, executed either on a University electronic information resource (“EIR”) or on a third-party EIR, that stores or processes the University’s Sensitive Information.

Production application means an application that is in use supporting a University business function.

4. PROCEDURES
4.1. For each application the IRM shall designate at least one application owner.

4.1.1. The application owner shall be an employee of the University.

4.1.2 The application owner shall be responsible for ensuring that the application complies with all relevant law and policy, including this Procedure.

4.1.3. The application owner may designate one or more application custodians.

4.1.4. The owner of an application may be a custodian of the application.

4.2. The IRM may consolidate or disapprove any application development or acquisition based on risk assessment, existing licensing agreements, or consolidation of University resources. The IRM may require that a particular acquisition or development effort be managed according to the Information Technology Department’s Project Management process. Any action taken by the IRM pursuant to this section may be appealed to the Executive VP of Finance and Administration.

4.3. The IRM and his or her designees are responsible for developing and maintaining a University Software Development Life Cycle ("USDLC") for all University application acquisition and development projects. At a minimum, the USDLC shall address the following areas: preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. The USDLC shall contain the following provisions:

4.3.1. There shall be a separation between the production, development, and test environments of an application, e.g., the establishment of separate test, development, and production servers

4.3.2. Test and development environments shall not use “live” data taken from production applications. Either fictitious data shall be used, or live data that has been sanitized or otherwise altered to protect Sensitive Information.

4.3.3. Production applications must restrict access to authenticated and authorized users and limit the privileges available to each user.

4.3.4. Production applications will encrypt all communications over non-University EIRs. For example, SFTP and HTTPS will be used instead of FTP and HTTP.

4.3.5. Production applications shall not store unencrypted confidential information on non-University EIRs. Instead, only the encrypted ciphertext of confidential information shall be stored on non-University
4.3.6. Applications shall not store passwords in plaintext. Only the encrypted ciphertext of a password may be stored, and that ciphertext has to be created with approved encryption methods.

4.3.7. Production applications will log significant application events including but not limited to: user account creations, modifications, and deletions; unsuccessful and successful logins and logouts.

4.3.8. The USDLC shall contain a code validation process to discover and remediate any code errors before an application is approved for production. The code validation process may include, but is not necessarily limited to, peer review and web application scanning.

4.3.9. Applications must be approved via the University’s Change Management Process before being placed into production.

4.2. An application’s owner shall be responsible for ensuring that the USDLC is observed when developing, acquiring, and placing the application in production.

4.3. All application development and acquisition shall comply with University Procedure 29.01.03.C2.22 “Software Licensing.”

5. CONSEQUENCES FOR VIOLATIONS

All University employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this University Procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this University Procedure are subject to loss of access privileges to University information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this Procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- Texas A&M System Policy
  o 01.03 Appointing Power and Terms and Conditions of Employment
  o 07.01 Ethics Policy, TAMUS Employees
  o 32.02 Discipline and Dismissal of Employees
  o 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  o 33 Employment, Standards of Conduct
• Texas A&M University-Corpus Christi Rule
  o 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  o 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation:  Information Security Office

Office of Responsibility:  Office of the Associate VP for Information Technology and CIO