29.01.03.C2.25 Exceptions to Required Risk Mitigation Measures  
Approved March 19, 2012  
Supplements System Regulation 29.01.03 and  
University Rule 29.01.03.C2

1. GENERAL

1.1 The purpose of this University Procedure is to provide a process whereby Owners and others may request exceptions to the required risk mitigation measures specified in the Information Technology Procedures (the 29.01.03.C2 series), and thus preserve the overall integrity and consistency of the University’s information security posture.

2. APPLICABILITY

2.1 This procedure applies to all users of the University Network, especially Owners.

3. DEFINITIONS

3.1 Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. PROCEDURES

4.1 Exceptions are of two types:

4.1.1 An exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type are to be initiated by an Owner or their designee.

4.1.2 Broader exceptions may be issued to address circumstances that span the University as a whole. Requests for exceptions of this type may come from any person, or may be initiated by the IRM. Exceptions of this type will be documented in each Procedure to which the exception applies.

4.2 Exceptions requested by an Owner must be submitted through the exception request form located at Information Security Office (iso.tamucc.edu). The request must contain the following:

4.2.1 Provision for which the exception is sought.

4.2.2 A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included.

4.2.3 Risk management rationale for the exception.

4.3 Each exception request will be reviewed by the IRM or designee. After any questions or concerns are addressed, the requestor will be notified as to whether
the request was approved or denied. A record of all requests and results will be maintained by the IRM or designee.

4.4 If the request is denied, a rationale for the denial will be supplied to the requestor.

4.5 If the request is approved:

4.5.1 The requesting Owner may be required to apply compensating security controls to mitigate any risk resulting from the exception.

4.5.2 An expiration date for the exception will be supplied to the requestor.

4.5.3 The request for the exception will be fully documented in the annual risk assessment in the form of a risk management decision by the Owner or their designee.

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 procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the IRM or designee.

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

- Texas A&M System Policy
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- Texas A&M University-Corpus Christi Rule
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Office

Office of Responsibility: Office of the Associate Vice President for Information Technology and CIO.