OIS 29 – Standard for Policy Exception and Risk Assumption

I. STANDARD STATEMENT

While it is the intent of the university that policies and procedures be adopted by the owners and stewards of information technology resources, there may be occasional exceptions to the application of policy due to technical, operational or administrative issues. In such cases the exception must be registered, the risk must be evaluated and documented, and formal approval must be obtained. The department requesting the exception will assume the risk(s) resulting from the exception.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. Exception Process
   1. The department requesting the exception must provide the following:
      a. Identification of the applicable policy
      b. Description of the requested exception
      c. The dates on which the exception will start and end
      d. Reason why the policy cannot, or should not, apply
      e. Description of the system impacted and the level of confidentiality of the data impacted
      f. Description of other risks that might occur
      g. Description of how the system will be monitored and compensating controls that will be established.

B. Requests for exceptions will be submitted to the Information Security Officer at informationsecurity@utsa.edu electronically by the head or chair of the responsible department, after consultation with the technical representative for that department or

unit. If the exception is denied, the issue may be escalated to the Chief Compliance Officer and Executive Director.

Title: OIS 29 – Standard for Policy Exception and Risk Assumption
Effective Date: January 10, 2012
Last Revised: August 4, 2020