Technology Services Security Exception Request Form

TEXAS A&M UNIVERSITY

GALVESTON CAMPUS®

Technology Services - Galveston has implemented security measures to protect our end users and their data on University issued devices. This includes full disc encryption, TAMUG Domain membership, end point protection, removal of administrative permissions, approved software use and patch management. If you have reason to believe that you cannot operate within these security measures and want to request an exception please fill out this form and **Email completed signed form to helpdesk@tamug.edu. **Download and open in Adobe to Digitally Sign****

Please refer to (TAMU Security Controls, TAMU SAP's) for further information about the various controls and SAP's that University personnel are required to follow.

If this request relates to computer that runs instrumentation, have you verified with the vendor that they do not support the latest operating system? We require an email from the vendor stating they do not support the latest operating system. Do not submit this request without that documentation.

Requestor Information

Name: _____ Date:_____

Phone: _____ Email: _____

Department: _____

Exception Information

Room Locations and DNS (Computer) Names of Machine(s):

Type of Request (place and X on your selection)

___ Retain Administrative Rights

___ Shared Account For Research Use

___ Request to Use Personal Device for University Business

___ Non-TAMUG Domain

___ Vulnerable Computer - Retain Network Access

___ SSN Retention

___ Significant IT Equipment (See Definition: Significant IT)

___ Other SAP or Security Control (TAMU Security Controls, TAMU SAP's)

Exception Description: Describe the exception you are requesting and the inability to utilize the existing standard, process or policy.

Business Justification: Describe the business reason for needing the exception.

Business Impact: Describe the business impact if the exception is not granted.

Compensating Controls: Describe what controls will be put in place to mitigate any exposure to the University, include initial and on-going controls. (Examples: patch updates, user accounts, passwords, drive encryption).

Data Sensitivity: Describe what type(s) of data will be hosted on the machine. Refer to TAMU Data Classification for definitions. TAMU Data Classification

Users: List current users of the machine and if staff, faculty or student.

By signing this document you are agreeing to implement any compensating controls required to protect University data from misuse and unauthorized access.

Requestor Signature: _____

Department Head Signature: _____

Technology Services Internal Use Only ISO

Approval: _____

CIO Approval: _____

COO Approval: _____