TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.06 Scheduled Maintenance and Change Management

First Approved: **March 28, 2013**
Revised: **June 22, 2017** *(replaces former TAMIU SAP 29.01.99.L1.30, Scheduled Maintenance)*
Next Scheduled Review: **June 22, 2022**

Procedure Statement and Reason for Procedure

The Information Resources infrastructure at Texas A&M International University (TAMIU) continues to expand and evolve. As the infrastructure becomes more complex, users depend on the continued stability of its networks, computers, and application programs. As the interdependences between Information Resources expand and become more complex, the need for a strong change management process is essential.

Managing all change is a critical part of stabilizing the Information Resources infrastructure. The TAMIU Office of Information Technology (OIT) requires a predefined maintenance window to perform planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur which may result in emergency changes.

The purpose of this SAP is to establish the process for managing changes in a rational and predictable manner so that the TAMIU community can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact to the user community and to increase the value of Information Resources. This SAP applies to all individuals who install, operate, or maintain TAMIU Information Resources. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

SCHEDULED MAINTENANCE
OIT has planned around TAMIU's academic calendar to designate a schedule for all Information Resources upgrades, changes, and maintenance which require an outage of a service. This schedule covers all the major planned maintenance days for the current fiscal year and will be posted on the TAMIU website.

UNSCHEDULED MAINTENANCE
In case an emergency arises (i.e., security vulnerability) where the risk of losing pertinent information is greater than the risk of loss from downtime, an exception can be made with approval of the Chief Information Officer (CIO).

CHANGE MANAGEMENT
The following change management protocols are highly recommend to be utilized by all TAMIU departments.

Normal Change – a modification to the hardware, operating system, or software that has the potential to impact normal operations. Items that are considered changes include, but are not limited to:

- installation or upgrades of server, networking, security hardware or software, including patches and fixes for the applications
- modification of hardware or software that affects the operation of multiple desktop computers connected to the TAMIU network
- modification of server, network, or security settings that affects access to IT information resources
- modification or enhancements to the physical environment that supports IT information resources

Standard Change – a change that is low risk, relatively common, and follows a procedure or work instruction. Reoccurring changes are treated as Standard Changes the first time that they occur. If successful, subsequent changes will be recorded as Service Requests (SR's). Examples of Standard Changes include:

- updates to or setup of a single desktop, creation of new file shares, or modification to permissions of existing shares
- installation, activation, or removal of network cable drops
- creation, modification, or deletion of accounts and mailboxes

Emergency Change – a change that must be implemented as soon as possible or one that bypasses the normal approval process. A change request should only be completed in response to an open and recorded incident. The change requestor/implementer must keep the Help Desk updated.

CHANGE MANAGEMENT PROCEDURES

All changes must be documented and submitted for approval prior to implementation. The following defines the procedure for documentation and approval:

1. The requestor/implementer requesting the change must fill out the Change Management Request to obtain approval.

2. The request will be submitted to the appropriate supervisor or manager for review. The supervisor or manager will ensure accuracy and completeness. Requests for change must be submitted to the supervisor or manager prior to the review date.

3. All changes must be forwarded to the Associate VP for Information Technology/CIO and/or the Information Security Officer (ISO) after approval of the supervisor or manager.

4. Whenever possible, changes to critical systems must be performed in a test environment prior to making changes in the production environment.

5. Once a major change has been performed, the Application Custodian and/or Owner will conduct a formal test to ensure its integrity.

6. Communication detailing impending change must be distributed to users prior to the change. The supervisor or manager should prepare such communication, and the director/supervisor for that area will be responsible for distribution of said communication. Typically, user notification may include an email or a posted message on the University portal.

7. On occasion, it may be necessary to implement emergency changes. If such an incident occurs, these changes must be documented.

8. An Incident Report must be completed for any unplanned incident affecting the system or network (i.e., power outages).

9. All changes affecting the physical environment of the computing facilities (i.e., air-conditioning, water, heat, plumbing, electricity, and alarms) will be planned with the approval of the CIO or designee.

10. Whenever possible, scheduled changes must coincide with the dates specified in the TAMIU standard operating procedure, Scheduled Maintenance, unless otherwise documented and planned.

11. All TAMIU information systems must comply with the Information Resources change management process outlined above.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310