Standard Administrative Procedure

29.01.99.L1.30  Scheduled Maintenance

Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: 01/24/15
Author: Office of Information Technology

General
The Information Resources infrastructure at Texas A&M International University (TAMIU) is expanding and continuously becoming more complex. There are more people dependent on the network, computers and application programs. As the dependency on Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time, each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur which may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

This SAP is a supplement to TAMIU’s 29.01.99.L1.06 Change Management SAP.

Applicability
The purpose of this SAP is to set the schedule for Information Resources maintenance and changes for the fiscal year. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources. TAMIU’s Scheduled Maintenance procedures apply to all individuals who install, operate or maintain Information Resources.

Scheduled Maintenance
The Office of Information Technology has planned accordingly with the 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 planned maintenance days for the current fiscal year. It is posted on the following website: http://uconnect.tamiu.edu. Monthly messages are also posted on UConnect.

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 CIO.
**Related Statutes, Policies, Regulations, Rules or Requirements**

TAC 202.75 Security Standards for Institutions of Higher Education

**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**

<table>
<thead>
<tr>
<th><strong>Office of Information Technology</strong></th>
<th><strong>Information Security Officer</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline: (956) 326-2310</td>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td>Killam Library 257</td>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Office Hours</strong></th>
<th><strong>IT Security Group</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
<td></td>
</tr>
</tbody>
</table>