Standard Administrative Procedure

29.01.99.L1.37 Clean Desk
 Approval date: 03/28/13
 Revision date: 01/24/13
 Next schedule review date: 01/24/15
 Author: Office of Information Technology

Standard Administrative Procedure Statement

General
In order to maintain a clean campus and protect University-sensitive information, it is essential to follow specific guidelines.

This procedure is established to:

- Reduce security incident threats
- Stress the importance of protecting office documents from malicious parties
- Set rules for a clean and safe environment

Applicability
The purpose of this SAP is to inform Texas A&M International University community of specific measures to take in order to maintain an overall positive environment. It applies equally to all University employees and on-campus third party contractors who work with sensitive information.

Definitions

Sensitive information – Information which is privileged or proprietary, whose unauthorized disclosure, alteration, corruption, loss or misuse can cause serious repercussions such as revenue loss, liability, loss of trust, or embarrassment to the institution affected.

Procedures and Responsibilities

Clean Desk
All University employees and on-campus third party contractors who handle sensitive information must adhere to the following practices to ensure protection from unauthorized access, alteration, exposure, or destruction. See 29.01.99.L1.31 Information Classification SAP.

1. All sensitive documents must be stored inside locked drawers when employees are away from their desks for extended periods of time (i.e. lunch break).
2. At the end of each working day, employees must clear their work stations of all office papers and sensitive materials, and they must ensure that desks and filing cabinets are locked.

3. Portable computing devices (i.e., laptops, tablets, etc.) and mass storage devices (i.e., CDs, DVDs, USB drives) must be secured in locked cabinets or drawers.

4. Whenever possible, University employees should scan documents and file them electronically in secure systems (i.e., Laserfiche, encrypted hard drive). Refer to 29.01.99.L1.24 Encryption SAP.

5. Sensitive documents that are no longer required must be shredded. This includes duplicates of forms with sensitive data.

Disciplinary Actions
Violation of this rule may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students.

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