General
With the increase of consumer smart communication devices, employees are using them for entertainment as well as productivity by connecting them to the Texas A&M International University (TAMIU) network. These devices may contain University-sensitive data and must be secured following specific policies.

Applicability
TAMIU has the responsibility of safekeeping information entrusted to it. This procedure establishes a University-wide rule for safeguarding TAMIU information on employee owned devices. It applies to all users of TAMIU Information Resources.

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Device Wipe: Restores device to factory default settings and erases all data from the device.

Exchange ActiveSync: Protocol that communicates over the web, designed for the synchronization of email, calendar, tasks, and notes from the University’s email server to a mobile device.

Personal computing device: Any device that is not property of Texas A&M International University and can receive or transmit data to and from IR. See portable computing devices definition for more information.


By connecting or “syncing” an employee owned device, the employee is responsible for any University information residing on the device and any potentially accessible information due to stored credentials in the personal computing device.

1. Employees must notify the Office of Information Technology as soon as possible if their device is lost, stolen or misplaced.
2. Employees have the option of sending a Device Wipe command which will automatically delete all data in the device.
3. If a lost or stolen device is believed to contain (or has the potential to contain) confidential information as defined in TAMIU’s 29.01.99.1.31 Information Classification SAP, the device may be wiped at the discretion of OIT.
4. The use of an employee device for state business purposes may require employee to surrender information within to open records requests.
5. Only devices that use the Exchange ActiveSync protocol are supported. POP/SMTP is not supported.
6. Encryption will be enabled on the device via ActiveSync policies.
7. A password or PIN must be set up in order to access the device and must be re-entered every fifteen minutes of inactivity.
8. All remote access to confidential information with personal computing devices must utilize encryption techniques that secure wireless transmission such as VPN.
9. TAMIU reserves the right to monitor the location of the personal computing device while on University premises. The TAMIU network may record time and position of the personal computing device. The information will be used to adjust network performance or locate the device in the event it contains TAMIU data.

**Disciplinary Actions**

Violation of this SAP 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. Additionally, individuals are subject to loss of TAMIU Information Resources access privileges and civil and criminal prosecution.

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

TAC 202.75 Security Standards for Institutions of Higher Education

**Appendix**

**References**
The State of Texas Information Act
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications
<table>
<thead>
<tr>
<th><strong>Contact Office</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of Information Technology</strong></td>
</tr>
<tr>
<td>Hotline: (956) 326-2310</td>
</tr>
<tr>
<td>Killam Library 257</td>
</tr>
<tr>
<td><strong>Office Hours</strong></td>
</tr>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
</tr>
</tbody>
</table>