## Standard Administrative Procedure Statement

### General
Technical support staff, security administrators, system administrators and others, may have Information Resource physical facility access requirements as part of their function. The granting, controlling and monitoring of the physical access to Information Resources facilities is extremely important for an overall security program.

### Applicability
The purpose of this SAP is to establish the rules for the granting, controlling, monitoring and removal of physical access to Information Resource facilities. It applies to individuals within Texas A&M International University (TAMIU) who are responsible for the installation and support of Information Resources, individuals charged with Information Resources security, and data owners.

### Definitions

**Data Center:** The facility used to house servers and network systems.

**Information Resources (IR):** Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

**Office of Information Technology (OIT):** The name of the TAMIU department responsible for computers, networking and data management.

### Procedures and Responsibilities

1. Physical Access

   1.1 All Information Resources must be physically protected based on risk in accordance with associated risk management decisions as part of the overall TAMIU security program.
1.2 Physical access safeguards help to establish best practices for the appropriate granting, controlling, and monitoring of physical access for all facilities supporting Information Resources. Physical access safeguards include the following:

1.2.1 All facilities supporting Information Resources must be physically protected in proportion to the criticality and confidentiality of their function.

1.2.2 All facilities supporting Information Resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.

1.2.3 Access to facilities supporting Information Resources will only be granted to authorized personnel of TAMIU and other contractors or personnel whose job responsibilities require such action.

1.2.4 Access cards and/or keys must not be shared with others.

1.2.5 Access cards and/or keys and badges that are no longer required must be returned to the responsible department contact. All returned access cards must be forwarded to Campus Card Services as soon as possible. Cards must not be reallocated to another individual, thereby bypassing the return process.

1.2.6 Lost or stolen access cards and/or keys will have access removed and must be reported to TAMIU’s ISO as soon as possible.

1.2.7 Access and log records for facilities supporting Information Resources are the responsibility of the department that manages the facility.

1.2.8 The department in charge of facilities supporting Information Resources must be notified within 3 business days if individuals who had access to these facilities should no longer need access due to a change in roles, completion of contract, or other cause that negates their need for further access.

1.2.9 Visitors must be escorted in controlled areas of facilities supporting Information Resources.

1.2.10 The department in charge of facilities supporting Information Resources must review access records on a periodic basis and investigate any unusual access.

1.2.11 Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

1.2.12 All physical security systems must comply with applicable regulations, including but not limited to, building codes and fire prevention codes.

1.2.13 Physical access to all Information Resources restricted facilities must be documented and managed.

1.2.14 All IR facilities must be physically protected in proportion to the criticality or importance of their function at TAMIU.

1.2.15 The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.
1.2.16 Requests for access must come from the applicable TAMIU data/system owner.

1.2.17 Cards and/or keys must not have identifying information other than a return mail address.

1.2.18 All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log.

1.2.19 Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

1.2.20 The person responsible for the Information Resources facility must remove the card and/or key access rights of individuals who change roles within TAMIU or are separated from their relationship with the University.

**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

---

**References**

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>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline: (956) 326-2310</td>
</tr>
<tr>
<td>Killam Library 257</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Information Security Officer</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Office Hours</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ITSecurity Group</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
</tbody>
</table>