Standard Administrative Procedure

29.01.99.L1.07 Email

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

---

**Standard Administrative Procedure Statement**

**General**
Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable State resources. This procedure is established to:

- ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- establish prudent and acceptable practices regarding the use of email.
- educate individuals who use email on their responsibilities associated with such use.

**Applicability**
The purpose of this SAP is to establish the rules for sending, receiving, or storing Texas A&M International University (TAMIU) electronic mail. This SAP applies to all individuals granted access privileges to any TAMIU Information Resource with the capacity to send, receive, or store electronic mail.

---

**Definitions**

**Confidential:** 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).

Examples of “Confidential” data may include, but are not limited to the following:

- Personally Identifiable Information such as: a name in combination with Social Security number (SSN), Date of Birth (DOB) and/or financial account numbers
- Banner ID in combination with Social Security number (SSN), Date of Birth (DOB) and/or financial account numbers
- Student Education Records
- Intellectual Property such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records (as defined by HIPAA)
**Electronic mail (email):** Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

**Electronic mail system:** Any computer software application that allows electronic mail to be communicated from one computing system to another.

**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.

---

### Procedures and Responsibilities

#### 1. Email Usage Procedures

1.1 Email must be used in a manner that achieves its purpose without exposing TAMU to any technical, financial, or legal risks.

1.2 TAMU has implemented an automated email retention schedule on the email servers that is based on the following:

   1.2.1 All messages in every folder stored on the email server that are at least 30 days old (based on received date), will be automatically and permanently deleted unless archived.

   1.2.2 Messages in the Deleted Items folder will be permanently deleted after 24 hours.

   1.2.3 Users are responsible for archiving important documents. Archiving is recommended every 14 days.

#### 2. Email

2.1 The following activities are prohibited:

   2.1.1 Sending email that is intimidating or harassing.

   2.1.2 Using email for conducting non-approved private commercial purposes.

   2.1.3 Using email for purposes of political lobbying or campaigning.

   2.1.4 Violating copyright laws by inappropriately distributing protected works.

   2.1.5 Posing as anyone other than oneself when sending email, except when authorized to send messages to another individual while serving in an administrative support role.

   2.1.6 Using unauthorized email software such as Thunderbird, etc.

2.2 The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
2.2.1 Sending or forwarding chain letters.

2.2.2 Sending unsolicited messages to large groups except as required to conduct University business.

2.2.3 Sending excessively large messages.

2.2.4 Sending or forwarding email that is likely to contain computer viruses.

2.3 All user activity on TAMIU Information Resources assets is subject to logging and review. There should be no expectation of privacy.

2.4 Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of TAMIU unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing TAMIU. An example of a simple disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer."

2.5 Individuals must not send, forward or receive confidential or sensitive TAMIU information through personal email accounts (See 29.01.99.L1.31 Information Classification SAP). If transmission of sensitive information to third parties is absolutely necessary, it must be secured (e.g., Filex, file encryption) and sent to their official, individual company/organization email account.

2.6 TAMIU email accounts are the official communication channel for all University business. Users must not use non-TAMIU email accounts for this purpose. Examples of non-TAMIU email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet service providers.

**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**

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 Publication

<table>
<thead>
<tr>
<th>Contact Office</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>