SUBJECT:	CATEGORY:	NO.
Mobile Device Access	**Information Management**	**808**

PREAMBLE

Mobile devices are a valuable tool in conducting business. The purpose of this policy is to define the accepted practices, responsibilities and procedures with respect to providing access for mobile devices.

The primary use of SIAST's email system is for business and educational purposes. Limited, occasional or incidental use for personal activities is acceptable, provided the privilege is not abused. Authorized users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the Internet are not secure and may be intercepted, and that email is subject to the provisions of The Local Authority Freedom of Information and Protection of Privacy Act. SIAST's existing policies Appropriate Use of Information Technology Resources Policy 801 and Harassment and Discrimination Policy 601, also apply to conduct while using SIAST's email system from a mobile device.

POLICY

Mobile devices will be allowed to connect to SIAST's email system to access services such as email, calendar, contacts and tasks.

Scope

This policy applies to all authorized users of SIAST's computer and network services, including, but not limited to, students, faculty and staff.

Privacy

SIAST respects the privacy of authorized users. However, any electronic record created on a SIAST computer or sent through the SIAST network is considered to be the property of SIAST. Please refer to the Record Retention and Disposal Policy O-5.3 for more information.

DEFINITIONS

Mobile Device

A mobile device is a smartphone or tablet computer that allows users the ability to connect to SIAST's email system.

Microsoft Exchange ActiveSync
A protocol that allow mobile devices to connect and synchronize to mailboxes within SIAST's email system.

Forwarding Email
Automatically sending email received at one address to another address.

PROCEDURES

Usage
Authorized users are responsible for all email sent from their individual user name, and should take appropriate precautions to ensure that their password is changed regularly and is not shared with anyone.

The following requirements must be adhered to for use of mobile devices:

1. **All Devices**
   - All mobile devices that are connected to SIAST's email system must have a password.
   - All mobile devices that are connected to SIAST's email system must be able to be remotely wiped (erased) in the event the device is lost or stolen.
   - All support for mobile devices will be handled by the service provider.
   - ITS HelpDesk support for mobile devices is limited to providing assistance for connecting to SIAST's email system.

2. **SIAST Owned Devices**
   - All employees must be authorized for a SIAST supported mobile device through the Mobile Communications Device Authorization Form. Please refer to the Mobile Communication Devices (MCD) Usage Policy 807 for more information.
   - Any SIAST owned mobile device that supports ActiveSync can be connected to SIAST's email system, provided they meet all requirements identified under point 1.0 All Devices.

3. **Employee and Student Personal Devices**
   - Any employee and student owned personal mobile device that supports ActiveSync can be connected to SIAST's email system, provided they meet all requirements identified under point 1.0 All Devices.
   - Students are also permitted to forward their SIAST email to an external email address in order to retrieve SIAST email from a personal mobile device.
   - If an employee ceases employment with SIAST and has a mobile device connected to the SIAST's email system, SIAST reserves the right to remotely wipe and erase the data from the mobile device.

4. **Device Backups**
   - Users are responsible for backing up all personal data and information on their personal mobile device. SIAST cannot be held liable for erasing user content and applications when it is deemed necessary to protect enterprise information assets or if a wipe is accidentally conducted.

5. **Instructions and Assistance**
   - For instructions and assistance on how to configure your mobile device to SIAST's email contact the SIAST HelpDesk.
   - For instructions and assistance on how to forward your SIAST email to an external email address contact the SIAST HelpDesk.

RELATED POLICIES/DOCUMENTS

807	Mobile Communication Devices (MCD) Usage Policy
801	Appropriate Use of Information Technology Resources Policy
809	Record Retention and Disposal Policy
601-G	Harassment and Discrimination Policy

APPLICABLE LEGISLATION OR REGULATIONS

The Local Authority Freedom of Information and Protection of Privacy Act

AMENDMENT HISTORY

1. Original issue date: June 4, 2014
2. Scheduled review date: June 2019