



SUBJECT: Information Technology Security	CATEGORY: Information Management	NO. 806
---	--	-----------------------

PREAMBLE

SIAS makes information technology infrastructure available to its students and employees. To ensure the integrity and performance of the infrastructure, a common set of security standards, procedures and guidelines are required to protect SIAS's data, applications and technology.

POLICY

Information Technology Services, in consultation with major stakeholders, defines and maintains a common set of procedures and guidelines to ensure the security of SIAS's data, applications and technology infrastructure. Any person accessing the SIAS information technology infrastructure must adhere to all security procedures and guidelines.

PROCEDURES

SIAS's Information Technology security procedures will be maintained within the following security categories.

1. Identification Defines processes and practices to verify the personal identity of those accessing the information technology infrastructure.
2. Authorization Defines processes and practices to assign the level of individual access to the information technology infrastructure in accordance with the rights granted by the custodian of the resource.
3. Safeguards Defines processes and practices that protect the integrity of the information technology infrastructure.
4. Compliance Defines process and practices to detect violations of this policy which put the information technology infrastructure at risk.

Approved by: Board of Directors	Prepared by: Information Technology Services	Date Issued: November 26, 2012	Supersedes/New Supersedes	Page 1 of 6 #806
--	--	---------------------------------------	----------------------------------	----------------------------

Specific guidelines related to this policy and related procedures can be located in the Information Technology Services section of the SIAST portal.

Identification Procedures

Purpose

This procedure defines processes and practices to verify the personal identity of those accessing SIAST's data, applications and technology infrastructure.

1. User Accounts

- 1.1. Information Technology Services is responsible for maintaining an automated user account creation process to ensure username and password uniqueness across the common SIAST domain. Each student and employee will be automatically assigned a unique SIAST user account once they become officially associated with SIAST. The person assigned to the account is responsible for its use.
- 1.2. Programs maintaining their own student user account process may define and manage these accounts according to their programs requirements. The program is responsible to ensure these user accounts are unique within each fully qualified domain.
- 1.3. SIAST user accounts are not to be reused.
- 1.4. Associate faculty or guest lecturers may be assigned a SIAST user account as required upon request to the SIAST helpdesk from an authorized employee. For purposes of this procedure, requests from program heads or deans (or equivalents) would be considered authorized requests. The employee authorizing these accounts must inform the Helpdesk when the accounts are to be disabled.
- 1.5. General purpose use of generic or guest user accounts for access to SIAST services is prohibited. In cases where special or short term access is required, generic or guest accounts may be created. In such cases, a SIAST employee will be designated as responsible for its use. These accounts must be disabled when not in use. The employee responsible for these accounts must inform the helpdesk when the user accounts are to be disabled.
- 1.6. Student SIAST network shares and email access will be disabled upon graduation or after fourteen (14) months of inactivity. Student user accounts will remain active for access to the SIAST portal. Programs can request student SIAST user accounts be disabled at anytime. Programs maintaining

Approved by: Board of Directors	Prepared by: Information Technology Services	Date Issued: November 26, 2012	Supersedes/New Supersedes	Page 2 of 6 #806
------------------------------------	--	-----------------------------------	------------------------------	------------------------

their own student user account process may define and manage these accounts according to their programs requirements.

- 1.7. Employee network shares and email access will be disabled as part of the Human Resources termination process. The employee user account will remain active for access to the SIAST portal.
- 1.8. Former SIAST employees re-employed by SIAST as a consultant may regain access to their network share and email upon approval of the provost and vice-president, academic or the vice-president, administrative services.

2. Passwords

- 2.1. Each user account must have a password associated with it.
- 2.2. All passwords must be treated as sensitive, confidential SIAST information. User accounts and passwords must not be shared with anyone, including Information Technology Services staff.
- 2.3. Passwords must not be written down, inserted into email messages or distributed in any other forms of electronic communication.
- 2.4. General purpose user accounts must have strong passwords consisting of a minimum of 8 characters in length.
- 2.5. Special purpose accounts or those accounts used to access restricted services may have different password minimum length and password composition requirements, depending on the service.
- 2.6. At a minimum, general purpose user account passwords must be changed every 4 months. All system-level passwords (e.g., administrator, application administration accounts, etc.) must be changed on a monthly basis, at a minimum.
- 2.7. Users with direct access to the Banner system are required to change their Banner password every 60 days and may not reuse a password within a 24 month period.
- 2.8. Applications requiring user authentication via a password must ensure the application supports authentication of individual users, not groups, and does not store the password in clear text or any easily reversible form.
- 2.9. Anyone suspecting that an account or password has been compromised should report the incident to the helpdesk immediately.

Approved by:	Prepared by:	Date Issued:	Supersedes/New	Page
Board of Directors	Information Technology Services	November 26, 2012	Supersedes	3 of 6 #806

- 2.10. Additional information and recommendations regarding proper password development and maintenance can be found in the SIAST Password Guidelines document located on the SIAST portal.

Authorization Procedures

Purpose

This procedure defines processes and practices to assign the level of individual access to SIAST's data, applications and technology infrastructure, hereafter referred to as information technology resources, in accordance with the rights granted by the custodian of the resource.

For purposes of this procedure, custodians are defined as the programs, departments or individuals who are responsible for the day to day operation, support and reliability of the data, applications and technology infrastructure under their control.

1. Custodians will be identified and assigned to manage access to all information technology resources. Custodians are responsible for reviewing and approving all requests for access to, or changes in access to resources under their control.
2. Access to SIAST information technology resources will be authorized on a 'least privilege required' basis. That is, account privileges will be set at the minimum level required to allow the user assigned to the account access to the resources they are authorized to use.
3. Custodians authorized to utilize enhanced account privileges must use these privileges only for the purpose intended.
4. Access to information technology resources will be assigned by groups and/or roles and not by individuals.
5. Custodians are responsible for reviewing and updating access privileges and group/role assignments to their information technology resources on a regular basis.

Safeguards Procedures

Purpose

This procedure defines processes and practices to protect the integrity of SIAST's data, applications and technology infrastructure.

To support teaching activities, programs responsible for operating and supporting their own servers and network equipment may define their own access and configuration procedures providing these procedures do not put the SIAST wide infrastructure at risk.

Approved by:	Prepared by:	Date Issued:	Supersedes/New	Page
Board of Directors	Information Technology Services	November 26, 2012	Supersedes	4 of 6 #806

1. Network Access

- 1.1. All perimeter network access points, whether wired or wireless, must be registered with Information Technology Services and be isolated from the SIAST network by properly configured firewalls.
- 1.2. Information Technology Services is responsible for allocation of all SIAST network addresses. Programs assigned a block of network addresses are responsible for management and use of addresses under their control.
- 1.3. All network traffic transporting user names and/or passwords must be encrypted.
- 1.4. Access to SIAST data from locations outside of the SIAST network will be encrypted via SSL or other appropriate secure access methods.
- 1.5. Unless under the supervision of faculty members or lab managers, computer labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact or have the potential to impact the SIAST network and/or non-SIAST networks.

2. Equipment Configuration & Management

- 2.1. Default system privileged accounts on servers and network equipment must be reconfigured or disabled before installation on the SIAST network.
- 2.2. All production servers and network equipment must physically be located in an access-controlled environment. For purposes of these procedures, production servers and network equipment are defined as any equipment providing services to students or employees that are normally expected to be available during SIAST operating hours.
- 2.3. Virus, malware and security updates must be installed on servers and network equipment as soon as practical, the exception being when immediate application would interfere with SIAST business or teaching requirements. Custodians responsible for servers and network equipment must have processes in place to stay current with virus, malware and security updates.
- 2.4. Unsecured services or protocols must be disabled or replaced with more secure equivalents whenever such exist.
- 2.5. Custodians responsible for servers and network equipment must have processes in place to review security incidents. The custodian is responsible to ensure corrective measures to prevent or mitigate further risk related to any security incident are implemented as soon as possible.

Approved by: Board of Directors	Prepared by: Information Technology Services	Date Issued: November 26, 2012	Supersedes/New Supersedes	Page 5 of 6 #806
------------------------------------	--	-----------------------------------	------------------------------	------------------------

- 2.6. Custodians responsible for servers and network equipment must provide Information Technology Services with an emergency contact.
- 2.7. In the event of a security emergency, Information Technology Services reserves the right to direct any custodian responsible for servers and network equipment to remove or shutdown any device as required.

3. Server Backups

- 3.1. Custodians responsible for server and network equipment must establish and maintain backup/recovery processes and procedures to safeguard the data held within.

Compliance Procedures

Purpose

This procedure defines process and practices to detect violations of SIAST Information Technology security policies which may place SIAST’s data, applications and technology infrastructure at risk.

- 1. Information Technology Services will conduct an annual security audit of the SIAST information technology infrastructure to ensure compliance with SIAST information technology security policy and associated procedures.
- 2. Results of the annual audit will be reviewed with custodians of the information technology resources. Information Technology Services will implement or assist with implementation of required changes to security process or practices as required.
- 3. An external security audit of the SIAST information technology infrastructure will be conducted every 3 years.
- 4. Failure to comply with SIAST Information Technology security policies and associated procedures may result in equipment being disconnected from the SIAST infrastructure. Individuals in violation of these policies and procedures may be subject to SIAST discipline procedures.

Approved by:	Prepared by:	Date Issued:	Supersedes/New	Page
Board of Directors	Information Technology Services	November 26, 2012	Supersedes	6 of 6 #806