SAIT

AD.2.10.1 PASSWORD GUIDANCE	
Section:	Administration (AD)
Subject:	Institute and Non-Institute Services
Legislation:	
Effective:	November 23, 2016
Revision:	April 21, 2021; October 11, 2023

PROCEDURE

APPROVED: _____

President and CEO

POLICY

The policy of the Board of Governors is to ensure the institute's information and related technology assets and service are managed effectively through a control framework.

PROCEDURE

PHILOSOPHY

Usernames and passwords are used to access SAIT's information and technology systems. Weak passwords are easily detected, and can put these systems at risk.

DEFINITION

Institutional data — Data that is created, collected, maintained, transmitted and stored by or for the institution to conduct institution business. It includes data used for planning, managing, operating, controlling or auditing institution functions and operations and as defined by the Data Governance Council/Steering Committee. It is not limited to data or information stored on centrally managed databases/servers. Data can also be stored on hosted services, individual desktops, paper files and electronic files such as spreadsheets.

Information and technology systems	Systems that include, for instance, network, email, web applications and services, and voice mail systems.

GOVERNING PRINCIPLES

1. This procedure applies to all individuals who have been granted access to SAIT information and technology systems, including but not limited to SAIT employees, contractors, and students. This excludes shared accounts.

2. Institutional data is one of SAIT's most important resources. It will be managed as a business-critical resource by following data management best practices and principles that safeguard the security of the data.

3. SAIT systems must be configured to follow the procedures outlined below. Systems that cannot be configured to follow these procedures must be identified and have compensating controls implemented.

PROCEDURE

1. Passwords shall not be reused. Initial/default passwords generated by SAIT should be changed.

2. Passwords must be kept secure and not written down and/or stored in an insecure manner.

3. Assigned usernames and passwords should never be shared with others. If someone requests or demands a password, refer that person to this procedure or ask that person to contact the Information Technology Services department, through the Service Desk.

4. If a user knows or suspects that the user's password has been compromised, the user must immediately report this to the Service Desk and must change the password.

5. The Service Desk is responsible for supporting users who wish to change their passwords but are unable to reset their SAIT Microsoft365 password using the self-serve password reset flow. The Service Desk can assist users (upon verification of end user identity) who request to have their passwords changed where the password has been forgotten or there is a problem with the password.

6. If a password needs to be reset by someone other than the user, the user's immediate supervisor must make the request to the Service Desk.

7. Password Standards

   a) Passwords must be at least twelve characters long and contain a combination of letters, numbers and symbols, or passphrase.

   b) Passwords must not be based on a user's easily accessible information or that of the user's family members, pets, friends or co-workers (for example, username, date of birth, address, phone number, SIN or any other unique identifying number or symbol).

   c) Passwords must not include common words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.

   d) Passwords must not employ commonly-used proper names, including publicly known fictional characters from books, films or places.

   e) Passwords must not be based on the school's or department's name or geographic location.

   f) Passwords used to gain access to SAIT systems should not be used as passwords to access personal systems, accounts or information such as home computing devices or personal web applications.

8. SAIT systems will be audited annually to ensure compliance with this procedure.

9. A user may be responsible for the consequences of someone else accessing and misusing the user's password.

10. Failure to comply may result in corrective action as set out in procedure HR 4.4.1 Corrective Action Procedures.

POLICY/PROCEDURE REFERENCE

AD.2.10 Information and Technology Management policy
AD.2.10.2 Technology Vendor Risk Assessment procedure

PROCEDURE