Policy Title:	**IT User Account Management**
Policy ID:	#6-602
Manual Classification:	Section 6 – Information Technology Services
Approved by Board of Governors (BoG):	October 2022
Original Approval Date:	May 2013
Effective Date:	November 2022
Next Policy Review Date:	November 2027
Contacts for Policy	Chief Technology Officer (CTO)

1.0 - Policy Overview

This policy (the "**Policy**") provides Fleming College with direction on the management of Information Technology (IT) user accounts to ensure individuals have the appropriate access to systems, software, and information to fulfil their role, while also ensuring that the College's information systems are appropriately protected and used.

2.0 - Purpose

This policy establishes the definitions, scope, and responsibilities relating to the consistent and appropriate management of IT user accounts provided by Fleming College. The College must keep an accurate and timely account registry to protect sensitive information, protect the integrity of our systems, and maintain cost-efficient licensing and infrastructure. This policy provides explicit lifecycle timelines for the phased closure of user accounts.

3.0 - Definitions and Acronyms

The following definitions and/or acronyms apply in this Policy:

Account Disable: When a user's account is placed into a disabled state to prevent any further access or use by the user. This is an interim state before deletion.

Account Expire: Accounts set to expire are effectively automatically disabled as of a known future date. This feature is used when access term limits are appropriate or required.

Admin Account: A special privileged user account that is assigned to staff (usually in an application or system administrator role) for the technical administration of college systems or applications. A separate admin account is often used to securely isolate the use of administrative privileges from a user's daily use primary Network Account, or when required by the system.

Application or System Administrator: A user who manages the upkeep, operation, and configuration of an electronic system or application. These users can be identified by having administrative privileges over the system or application.

AUP: College Policy #6-601 - Appropriate Use Policy

CTO: The Chief Technology Officer is the College's executive role responsible for the management of Information Technology at the College.

ERP: Enterprise Resource Planning (ERP) is a generic term used to refer to systems used by large enterprises to manage and integrate their core business process, such as Oracle PeopleSoft.

HR: Human Resources

IT: Information Technology

ITS: Information Technology Services is the full name of Fleming's IT Department

Multi-factor Authentication (MFA): An authentication method that requires the user to provide two or more verification elements to prove their identity to gain access to a system. E.g., a password and one-time code sent to the user.

Network Account: A user's primary account created by the ITS Department to provide access to ITS systems. Where supported as feasible to do so, college IT services are configured to support single sign-on (SSO) to a user's primary network account thereby limiting the number of login credentials needed to access most college systems.

Personal: In terms of an individual's electronic resources, the term personal means associated with or belonging to a specific Fleming User. E.g., personal college email account.

Service Account: Created by ITS to allow specific local services to be run or accessed. Service accounts must have an accountable administrative user or service owner.

Single Sign-on (SSO): An authentication service that allows users to use one set of centralized login credentials to access multiple services.

Staff Account: An account provided to an employee of the College identified by a unique employee ID.

Student Account: An account of a student at the College identified with a unique student number.

Student Employee Account: An account provided to a student that requires elevated access to systems in order to fulfill their employment duties at the College for a period of time defined in their employment contract.

Temporary / Guest Account: An account with limited access provided for one-time or short-term use, for a period defined when the account request is made.

Third-Party / Contractor Account: An account provided to third-party employees or contractors requiring access to college systems for a period of time defined when the account request is made.

User: A person that has been authorized to interact with an Information Technology system such as an application, device, database, website, or other resources.

4.0 - Scope

This policy applies to everyone with a Fleming College user account.

All systems owned and operated by Fleming College must have user accounts maintained in accordance with this policy.

The primary office of responsibility for this policy is the Chief Technology Officer (CTO).

This policy must be interpreted and applied in compliance with the College's obligations under all collective agreements. Nothing in this or related IT policies must be interpreted as limiting or amending the provisions of any collective agreement. To the extent that policies may conflict with the College's obligations under any collective agreement, the collective agreement prevails provided that its provisions do not conflict with FIPPA or PHIPA.

5.0 - General Principles

5.1 - Manager responsibilities:

Managers are responsible for establishing and managing the need, validity, and appropriate access of IT user accounts used by their staff. These responsibilities include:

a) Authorising access and privileges for their staff to access Fleming College IT systems and data within their responsibility as appropriate or required, either as a new user or as a change to an existing user's job role or employment status.

b) Notifying the Human Resources (HR) Department of employee employment status changes and ensuring the information is accurately reflected in the

College's ERP system.

c) Revoking user authorizations and privileges within their responsibility as appropriate.

d) Ensuring that breaches of this protocol occurring within their unit are reported, resolved, and referred to the ITS Department, and to participate in any potential ongoing investigation according to the Information Security Incident Management Operating Procedure #6-604C.

5.2 - Human Resources responsibilities:

a) Maintaining an accurate registry of employees along with their assigned roles and current employment status within the College's ERP system. Each employee record must be kept current with every change including role changes.

b) Responding to requests from ITS staff for reports on employment status changes including retirements, terminations, leaves, and layoffs.

5.3 - ITS Department, Application, and System Administrator responsibilities:

a) Using and maintaining any user information responsibly, confidentially and within the guidelines of this policy, the AUP, and any relevant legislation (FIPPA, PHIPA, PIPEDA).

b) Responding to user change requests in adherence to this policy referring any deviance from this policy to the CTO or delegated authority.

c) Creating, maintaining, disabling, and deleting user accounts and associated personal user resources within the guidelines and schedules of this policy.

d) Maintaining the practices as detailed in this policy, related operating procedures, and applicable ITS standards for passwords and privileged account management.

5.4 - User responsibilities:

a) Under the ITS Appropriate Use Policy (AUP), users are responsible for maintaining the security of their user account credentials (username, password, and associated multi-factor authentication (MFA) information), and the associated system/information access.

b) Users can provide proxy or share access, to their own personal network resources, with other Users via College IT systems. Users who provide and manage access rights to their personal network resources are fully responsible for any implications or impacts of their actions.

c) Before staff users leave employment or change job roles at the college, in consultation with their manager, they will make the appropriate arrangements for copying or otherwise making available, any electronic data stored in their personal network resource locations, that may be required by their department/school to continue operations in their absence or required for record retention/archival purposes. Once a staff member leaves the college their User account(s) will first be disabled, and subsequently deleted along with any personal network resources, in accordance with Appendix A - User Account Schedule.

5.5 - Lifecycle of Personal Electronic Resources

IT user accounts and associated electronic resources provided by the College are only authorized to conduct college activities. As user accounts are disabled and deleted in accordance with this Policy, the use of College IT resources for purposes not related to a user's role at the College is strongly discouraged.

The College will retain the contents of a user's personal network resources up until the time of account deletion in accordance with this policy.

6.0 – Operating Procedure

6.1 - Short Notice Account Secure

The purpose of a short notice account secure is to immediately revoke a user's access to IT systems. These requests need to be acted upon quickly in the best interests of the College, for example, in the event of a termination of employment. Such requests are sensitive and confidential in nature and as such must be made directly to the CIO or designate without submitting a written IT request ticket. Due to the sensitive nature of such an action these requests to disable accounts will only be supported from the following sources:

Staff – by the Vice-President HR or their delegated authority, or a member of the Senior Management Team.

Student – Dean, Student Services Leaders, HR human rights delegate, or a member of the Senior Management Team. In this event, the student rights and responsibilities process and procedure shall then be invoked.

6.2 - Disabling Accounts

User accounts are to be disabled before being deleted. Disabling an account forces inactivity which may be used as an indicator or trigger to schedule the subsequent account deletion. See Appendix A – User Account Schedule for account disable triggers and specific timing.

a) **Staff leaving employment** - Staff leaving employment from the college shall have their account disabled after a minimum period as specified in Appendix A – User Account Schedule, following their last day of active employment. It is the responsibility of the manager to inform ITS and HR of staff leaving their employ.

b) **Staff retirees** - In terms of user account management, staff retiring from the College will be treated the same as staff leaving employment by the College.

c) **Admin Account** - Admin Accounts are to be immediately disabled when the elevated administrative privileges are no longer required by the staff member, including when they leave the employ of the college or change job roles.

d) **Student not enrolled in courses** - Students that are not actively enrolled in timetabled courses, or otherwise academically active at the college, will have their account disabled after a minimum period as specified in Appendix A – User Account Schedule, following the date of the last timetabled course.

e) **Service Account** - Service accounts are to be immediately disabled when no longer required to run or operate the service.

f) **Account expiry** - Account expiry is set by ITS or system/application administrators to automatically disable an account with a known end of use or termination date. Student employee and third-party / contractor accounts will be configured with a future expiry date at the time of account creation. The expiry date may be changed as needed based on changes to employment or contract dates.

6.3 - Deleting Accounts

The following types of user accounts will be deleted after a minimum period of inactivity precipitated by the account disable action, both according to Appendix A – User Account Schedule.

- Students
- Staff
- Admin and Service Accounts
- Student Employee
- Third-party / Contractor

Deleting an account also includes the deletion of personal network resources belonging to or directly associated with the target user account.

6.4 - Returning users

Users who have been away from the College but return after their User is deleted will not have their account restored, they will be given a new account.

6.5 - Employee separation where the employee is also a student

Current employees who are also currently enrolled in an academic course at the College, if their employment with the College ends during the term of a course, they will be given a new Student Account.

6.6 - Student to Staff account conversion

If a student has completed their academic studies at the College is subsequently hired as an employee of the College, and their previous student account exists, (has not been deleted), then the new employee/former student, may be given the option to have their Student Account converted to a Staff Account.

By electing to have their account converted from student to staff, the new staff account and all associated personal network resources contained within at the time of conversion become governed by staff account policies.

If they choose not to have their Student Account converted, a new Staff Account will be provided.

The account conversion process is only permitted in one direction, from student to staff. For security reasons, an existing Staff Account can not be converted into a Student Account.

6.7 - Litigation Hold

Members of the College's Senior Management Team (SMT) will inform the CTO of any ongoing or potential litigation, or other exceptional circumstances, that require the preservation of data and record retention beyond the normal User account or other retention schedules.

User accounts will be placed on litigation hold upon approval of the CTO or designate.

User accounts, and their associated personal network resources, will be retained indefinitely while under litigation hold status, as an approved exemption from Appendix A – User Account Schedule. Depending on the circumstance, the target user may not be notified of the litigation hold being added, removed or current litigation hold status.

The CTO will review accounts under litigation at least annually to confirm if still required.

6.8 - Access to Personal User Account Resources by Others

See College Operating Procedure #OP 6-601, AUP and Accessing Another User's Data Procedure, for information and timelines related to this procedure. In terms of this policy:

a) Account disabled status is not a pre-condition for permitting access to personal user account resources by other individuals approved under OP 6-601.

b) Similarly, (self-provided or OP 6-601 approved), access to personal user account resources by other individuals does not prevent account and personal network resource deletion under this policy. Users who have been granted access to the personal resources of staff no longer employed by the College and require record retention beyond the deletion timelines described in Appendix A – User Account Schedule, are to contact CTO to request extended record retention as an exception to this policy.

7.0 - Related Documents

- *Personal Information Protection and Electronic Documents Act* (PIPEDA), SC 2000, c. 5
- *Freedom of Information and Protection of Privacy Act* (FIPPA), R.S.O. 1990 c. F. 31
- *Personal Health Information Protection Act* (PHIPA), SO 2004, c. 3, Sch A
- College Policy #1-111, Access to Information and Protection of Privacy
- College Policy #6-600, IT Policy Framework
- College Policy #6-601, IT Appropriate Use Policy
- College Operating Procedure #OP 6-601, AUP and Accessing Another User's Data
- College Operating Procedure #OP 6-604C, Information Security Incident Management

History of Amendments/Reviews

Date	Actions
March 2013	Original policy approved by BoG
October 2022	Policy reviewed and revised: changes to timing of disabling staff accounts, added criteria for disabling student accounts; approved by BoG

Appendix A - User Account Schedule

Account type/Activity	Account Action	Trigger	Timing
Student Accounts			
Student not enrolled in a College course	Disabled	Date since last timetabled course	After (16) months
Student account	Deletion	Account inactivity	After (8) months from account disable
Staff Accounts			
Staff leave college	Disabled	Employment end date	Immediate, if possible, maximum (1) week from the employment end date
Staff account	Deletion	Account inactivity	After (24) months from account disable
Other Account Types			
Admin and Service account	Disabled	When no longer needed	Immediate
Admin and Service account	Deletion	Account inactivity	After (6) months from account disable
Student Employee account	Expired	Employment end date set at account creation	Immediate, if possible, maximum (1) week from the employment end date
Student Employee account	Deletion	Account inactivity	After (24) months from account disable
Third-party account	Expired	Contract end date set at account creation	As per the predefined expiry date
Third-party account	Deletion	Account inactivity	After (6) months