Fleming College

SIR SANDFORD FLEMING COLLEGE POLICY MANUAL

Policy # 6-602 ITS User Account Management	
Classification: *Section 6 – Information Technology Services*	
Approved by: Board of Governors	Date: May 1, 2013 (BoG May 1, 2013 #11)
Replaces: NEW POLICY	
Next Policy Review: *2018*	Responsibility*:* Executive Leaders Team

Policy Statement

This policy guides the management of Information Technology user network accounts to ensure that individual users have the appropriate level of access to systems, software and information to fulfil their role and to ensure the College's information and systems are used appropriately. This policy ensures fair and consistent practices are followed when accessing individual user accounts and the information they contain, including the deletion of any data held in a user's personally assigned network space (H: drive) or email**.**

Purpose

This policy establishes the definitions, scope, and responsibilities relating to the consistent and appropriate management of IT User accounts provided by Fleming College.

Scope

This policy applies to everyone with a Fleming College IT Network user account

The primary office of responsibility for this policy is the Chief Information Officer.

Definitions

ITS: Information Technology Services, referring to the department responsible for information technology

HR: Human resources, referring to the department responsible for human resources

Network Account: A user network account is an IT account created by the IT Services department for the sole purpose of enabling employees and students of Fleming College to access IT systems and associated data enabling them to study and work at Fleming College as appropriate within their role.

Staff Account: This account applies to an employee of the College who is required to use ITS services in the course of their work. They are identified by a unique employee ID

Student Account: A Student of the College requiring access to College information, software applications and services as part of their studies. They are identified with a unique student number.

Student Employees: A Student user with a student number that requires elevated access to other systems in order to fulfill their employment duties at the College for a period of time defined in their employment contract.

College Affiliate Account: This account is created for individuals from partner organizations (e.g., High School / Dual Credit Students) for a period of time defined when the account request is made.

Third Party Contractor Account: This account is created for third party employees or companies

requiring recurring use of the College systems (e.g., Aramark, Omni, Consultants) for a period of time defined when the account request is made.

Temporary Account: An account with internet access and printing services enabled for a short term period defined when the account request is made.

Utility Account: Used by ITS to allow local administrative access to the logged in workstation in order to install specialist software etc.; usually associated with an employee of the College.

Admin Account: These accounts are typically associated with higher level privileges including local workstation administrator and directory administrator rights. Because of their level of access, these accounts are restricted to Fleming ITS staff or in the case of third party software the designated Manager of the area.

Account Secure: This term is defined as the users account password being changed to an unknown random password to prevent login access to the account. The account will still exist but no user will be able to login to that account. Un-securing the account will require the setting of a known password by ITS.

Account Disable: This term is used for a user's account being placed into a disabled state within the user directory. This state differs from expiry in that proxy access can still be granted to an email account or data. For example when a retiree leaves employment they may have email & data that is still pertinent to College business. It is the interim state in which a user account begins its migration to full termination and deletion.

Account Expire: Accounts set to expire are effectively closed for further use; services supplied to that account are unavailable. Account expiry is limited to non-personal accounts such as utility accounts, or 3rd party contract staff with a known termination date.

Account Deletion: At this stage the account credentials are deleted from active directory all email and personally assigned network space data is deleted. Data on public or group drives is the responsibility of the Department that uses such data and parameters on retention and storage of information can be found in Policy # 6-603 ITS – Data Retention and Disposition.

General Principles

1. Supervisor responsibilities: Administrative heads of schools/departments are responsible for establishing and managing the validity of IT user network accounts used by their staff. These responsibilities include:
   - Authorising access and privileges for members of their department in order to access Fleming College IT systems and data within their responsibility as appropriate or required, either as a new user or as an amendment of current user status.
   - Notification of renewing, retiring, and revoking user authorizations and privileges within their responsibility as appropriate.
   - Ensuring that breaches of this protocol occurring within their unit are resolved and/or referred to IT Services, as appropriate and to participate in any potential ongoing investigation.

2. Fleming College IT Services responsibilities include:
   - Using and maintaining any user information responsibly, confidentially and within the guidelines of this policy, the appropriate use policy, and any relevant legislation (FIPPA, PHIPA, PIPEDA).
   - Responding to user change requests in adherence to this policy referring any deviance from

this request to the CIO or delegated authority.
- Creating/maintaining and deleting user accounts and data within the guidelines of this policy.
- Maintaining the practices as detailed in this document.

3. Human Resources responsibilities include:
   - Advising ITS when employees are hired and who, as part of their job duties, require access to the services covered by this policy.
   - Processing in the HRIS system, regular and temporary staff and job changes as submitted by hiring leaders and HR staff, and related impacts to human resources and payroll.
   - Responding to requests from ITS staff for reports on employment status changes including retirements, terminations and layoffs.

4. User responsibilities include:
   - Under the ITS appropriate use policy, users are responsible for maintaining the security of their user network account credentials (username and password) and the associated access to data.
   - Users can provide proxy access to their own personal data to others via College IT systems. Users who provide proxy access to their email account and manage trustee rights to their own data in shared and personal drives are fully responsible for any implications or impacts from their actions.
   - ITS is not responsible for maintaining user account proxy/trustee rights access beyond providing 3rd party access to personal data as detailed in the procedures.
   - Before leaving the college users in consultation with their manager will make the appropriate arrangements for copying over the data to the appropriate archive (their own drive/shared drive). Once users leave the college their data will be deleted in accordance with this policy.

Operating Procedure

1. Access to User Accounts by Others

   Upon CIO/or designate approval, ITS will provide the following access services:
   - access to personally assigned network space and, or, create new space for local user
   - proxy access to email account and, or, create new email account
   - auto forwarding of email to another user (re pointing)

   Proxy access and auto forwarding of email will require the ITS team to access the account in question. Upon approval the access requester assumes responsibility to handle the data responsibly and with confidentiality. This access to the specified User Account data will be restricted to a limited time as specified in the schedule in the Appendix.

   Email/proxy/alias re pointing will be restricted to a maximum time as specified in the schedule in the Appendix.

2. Short notice account secure

   These requests are defined as requests that are needed 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 ticket.

   Due to the sensitive nature of such an action these requests to disable accounts will only be supported from the following sources:
   - Staff (Administrators, Support Staff and Faculty) – by the Vice-President HR or their delegated authority, or a member of the Executive Leadership Team.

- Student – Dean, Student Services Leaders, HR human rights delegate or the Executive Leadership Team. In this event, the student rights and responsibilities process and procedure shall then be invoked.

3. Automatic or scheduled disabling
   - *Staff retirees*
     Staff retiring from the College shall have their accounts disabled after a minimum period as specified in the schedule in the Appendix following their retirement date as advised by the Benefits Administrator within HR. The retiree will be informed of the impending closure by HR Benefits Administrator during the retirement engagement meeting.

   - *Staff leaving employment*
     Staff leaving employment from the college shall have their account disabled after a minimum period as specified in the schedule in the Appendix following their leaving date. It is the responsibility of the manager to inform ITS of staff leaving their employ.

   - *Account expire*
     Account expiry is limited to non-personal accounts such as utility accounts or third party contract staff with a known termination date. Expiry dates are set by ITS according to use. Maximum expiry date for non-student employees is specified in the schedule in the Appendix.. Student employees' expiry will be set separately for a period specified in the schedule in the Appendix.

   - *Account deletion*
     Student: Student accounts will remain active unless there is no login to directory services or email for a period specified in the schedule in the Appendix after which the account will be disabled by ITS. Personally assigned network space and email data shall be deleted. Student employees will come under the same governance as Staff.

     Staff: Staff accounts will remain active unless there is no login to directory services or email for a period specified in the schedule in the Appendix after which the account will be disabled by ITS. Personally assigned network space and email data shall be deleted.

     3 Party - 3rd party/Contractor accounts will remain active unless dormant for a period specified in the schedule in the Appendix after which all account and email data shall be deleted.

     Utility: Utility accounts are deleted as appropriate under bi-annual reviews.

4. Removal/remapping of public drives
   A ticket will be submitted detailing the request from the user's immediate manager and/or the Vice President of HR or their delegated authority.

5. Returning users
   Users who have been away from the College but return after their personally assigned network space data is deleted will not have their accounts reactivated. They will be given new accounts.

Related Documents

- ITS – Data Retention and Disposition, *Policy #6-603*
- FIPPA, PHIPA, PIPEDA

Appendices

Appendix 1: User Account Policy Schedule

Monitoring of Operating Procedure

Next Review: *2016*
Responsibility of: *Chief Information Officer*

Procedure Review Summary:

Section and Month date, year	Person/Department/Committee
Section and Month date, year	Person/Department/Committee

User Account Policy Schedule

Account type/Activity*	Account status	Trigger*	Duration
Proxy access to account	Access to account by others	CIO (or designate) approval	(1) month
Email/proxy re pointing	Access to email by others	CIO approval	(3) months
Retirees account	Account disabled	Retirement date	(6) weeks from retirement date
Staff leave college	Account disabled	Employment end date	(6) weeks from employment end date
Third party account	Account expired	Set at account creation.	At completion of agreement
Non student employee	Account expired	Employment end date	(6) months from employment end date
Student employee account expire	Account expired	Employment end date	After (12) months
Student Account	Account deletion	Account inactivity	After (12) months
Staff Account	Account deletion	Account inactivity	After (24) months
Third party	Account deletion	Account inactivity	After (1) month

* For a complete description of user account activities and triggers, see parent Policy document (Policy 6-602)

Created: January 10, 2013
Approved Revision: