Fleming College

LEARN | BELONG | BECOME

ADMINISTRATIVE OPERATING PROCEDURE

Procedure Title: AUP and accessing another user’s data	
Procedure ID:	#6-601 OP
Approved by Executive Leaders Team:	*Original*: ELT *Revisions: N/A*
Effective Date:	June 1st 2017
Next Review Date:	*Scheduled for 2 years*
Monitoring Responsibility:	CIO / ITS
Linked to a College Policy:	x Yes # 6-601 *Information and Communications Technology (ICT) Appropriate Use Policy* ☐ No

Policy Statement

The College’s Appropriate Use Policy (AUP) outlines exceptions to user privacy and subsequent access to a user’s data by others.

Under Authorised Use Policy 6-601 > Section: 1.1

Exceptions to user privacy and subsequent access to user data exists as follows:

- To engage in technical maintenance repair and management
- To meet a legal requirement to produce information, including by e-discovery
- To ensure continuity of work (e.g. employee is sick or injured and work needs to be retrieved)
- To prevent misconduct and ensure compliance with the law

  In such cases access to personal data shall only be given with due diligence of requesting such access via the CIO or in their absence a delegated authority.

This procedure defines the actions and responsibilities of the College users when a request is made to access another users’ account data. Such evolutions are often highly technical in nature. To maintain clarity within a complex subject, the technical aspects of the work are defined in appendix A of this document

Scope

In Scope: The granting of a privacy exception for one employee to access the data resources of another employee, such as email, H: drive, etc. These types of requests are not uncommon as they often occur when an employee is unexpectedly away from the workplace or when an employee leaves the College.

Out of Scope: This document does not describe the ITS protocol as it pertains to legal discovery, legal compliance, litigation hold, employee access termination upon employment termination, any sensitive employment issues, or technical maintenance repair & management of IT resources that contain or handle personal user data.

Operating procedure

Each request can be highly specialised in nature covering a multitude of scenarios and technical solutions to achieve. Therefore the review and approval of such requests must come from a position that has the authority and context within which to balance policy vs business need. That is the CIO or delegated authority.

This procedure is built on the premise that no single user has absolute authority and ability to access another users' data. i.e. as the Policy holder on behalf of the College, exceptions are approved by the CIO but they should not have access to the actual tool set to conduct the search themselves.

The College will operate under the following principals

1. No single user has complete authority to approve and conduct a search

2. Requests for access to another users account may only come from an administrator.

3. Approval for access may only be granted by the CIO or in their absence their delegated authority after establishing the validity and need of the request.

4. If access is declined, a requestor should seek recourse via their ELT representative.

5. ITS will assess the request and only provide the minimum access to achieve the request

6. The administrator's actions when accessing another users data are subject to the Appropriate Use Policy

7. ITS will provide an auditable record of the actions taken, monitor status, and remove access within stated time lines

8. The user whose personal data has been accessed will be notified by ITS defining what access was given, to who, and why.

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
- forwarding of email from one personal account to another
- monitoring and follow up to each request

Changes in technology are commonplace and services will adapt as tools and skillsets allow. Therefore the full procedure of ITS actions are detailed in annex A.

Related Documents

- College Policy #6-601, *Information and Communications Technology (ICT) Appropriate Use Policy*

Appendices

Forms that are generated by this operating procedure are listed and included with the document.

- Appendix A – Protocol for Proxy Access to Personal User Data

\

History of Amendments/Reviews:

Section(s)	Date	Comments
e.g. New procedure	June 2017	• ELT approval of operating procedure (date of meeting)
e.g. Procedure reviewed and revised	Month year	• ELT approval of operating procedure (date of meeting)

Appendix A to Operating Procedure 6-601 OP: ***Protocol for Proxy Access to Personal User Data***

AUP: Protocol for Proxy Access to Personal User Data

Document Information

Document Title	AUP: Protocol for Proxy Access to Personal User Data
Department	ITS
Owner	Roger Fitch, CIO
Author(s)	Paul Marchant, ITS Operations Manager
Publish Location	https://department.flemingcollege.ca/its/attachment/###/download
Revision Date	13-May-2016
Version #	1.0
Document Status	PUBLISHED

Document History

Version	Date	Details
1.0	13-May-2016	Initial version. /pm

Contents

1 Objectives

This protocol is linked to College procedure <insert number here> and defines the specific actions ITS services take when granting an exception to User privacy for business continuity reasons.

In Scope: This document describes the ITS protocol & controls used when implementing proxy access to personal data. For example, the granting of a privacy exception for one employee to access the data resources of another employee, such as email, H: drive, etc. These types of requests are not uncommon as they often occur when an employee is unexpectedly away from the workplace or when an employee leaves the College.

Out of Scope: This document does **not** describe the ITS protocol as it pertains to legal discovery, legal compliance, litigation hold, employee access termination upon employment termination, any sensitive employment issues, or technical maintenance repair & management of IT resources that contain or handle personal user data.

2 Protocol Overview

Protocol Name:	**AUP: Protocol for Proxy Access to Personal User Data**
Owner:	CIO, Roger Fitch
Points-of-Contact:	IT Operations Manager, Paul Marchant IT Customer Services Manager, Barry Knight

2.1 Roles & Constraints

- **Requestor:** a **College Administrator** who initiates the request for an exception to the privacy of a network user.

- **Source User:** the network user account of a real-person whose personal user data is being accessed by others.

  - If the Source User is an employee of the College, the Requestor must be the manager of the Source User, either directly or by organizational hierarchy.
  - If the Source User is a student or third-party, the CIO will decide who is an appropriate Requestor is based on the specific circumstance.

- **Target User(s):** the user(s) who is/are receiving the privileged to access the personal data of the Source User. May or may not be the same as or include the Requestor.

- **NSA:** ITS staff who implements the systems changes to provide/facilitate access and subsequent removal.

- **Telecom Administrator:** ITS staff who implements the voice-mail password reset deliverable as required.

- **CIO (or designate):** approver of user privacy exception. In the CIO's absence, designated approvers are the Director of ISG or the VP Finance.

- **IT Customer Services Manager:** monitor and communicates the upcoming expiration of the privileges to the Requestor and Target User(s).

2.2 Privilege Access Deliverables

Depending on the circumstance and specific business continuity need, (e.g. redirecting new inquiries versus access to historical data), the Requestor, (in consultation with ITS as needed), indicates which type of access is needed:

- Provide the Requestor with a **new voice-mail password** in order to change greeting & access voice-mails.
- Email Server Administrator (NSA) configures the **out-of-office email responder**, (internal and/or external incoming emails) to
  the message(s) provided by the Requestor.
- Email Server Administrator (NSA) configures an automatic **forward (and retain) a copy of new incoming email** to alternate recipient(s) as specified by the Requestor.
- **Read-only access to a user's H:\ drive** for Target User(s).
- **Proxy access to a user's email mailbox** for Target User(s), excludes "Send As" abilities.

2.3 Protocol Oversight

At the ITS Leaders weekly meeting, the AUP Request bucket within the ticket system will be reviewed with respect to:

- New AUP Requests
- Requests pending CIO approval
- Upcoming access expirations
- Timely removal of access privileges

3 Process Steps

1. Request: The Requestor initiates the request, expressing the need & circumstance for the Target User(s) to be granted specific Privilege Access Deliverables belonging to a Source User.

2. Handling: The request should come in the form of an email to aup@flemingcollege.ca in order to automatically create a new ticket in the AUP bucket of the IT Ticket system. An NSA will be set as the owner of the ticket and responsible for bringing the in-queue request to the attention of the CIO. The IT Customer Services Manager will be set as a watcher of the ticket.

   (If the CIO or one of the IT Leaders is emailed directly regarding an AUP request, it will be forwarded to this email address. If request comes in as a regular ITS Support Ticket it will be moved to the AUP bucket.)

3. Approval: The CIO or designate will indicate to the NSA in writing if approval is granted.

4. Implementation: The NSA will proceed to implement the approved access & log via the ticket the particulars of how the access was granted and the date it was given. The NSA will advise Requestor & Target User(s) of the newly provisioned access and provide them with instructions on how to access/connect to the Source User's data resources.

   Note: If a voice-mail password reset is required, the ticket will be assigned to the Telecom Administrator to implement this deliverable and advise only the Requestor of the new voice-mail password. Once this portion is complete, the Telecom Administrator will assign the ticket back to the NSA.

5. Plan Follow-up: The NSA will set:

   a. Status to Waiting for Reply
   b. Ticket Owner as IT Customer Services Manager
   c. Hard Due Date will be set by the NSA with the appropriate duration:

   - 1 month for full proxy account access

   - 3 months for mailbox proxy of forwarding access

6. Access Expiration Notice: Time elapses and 5-business days before Hard Due Date arrives:

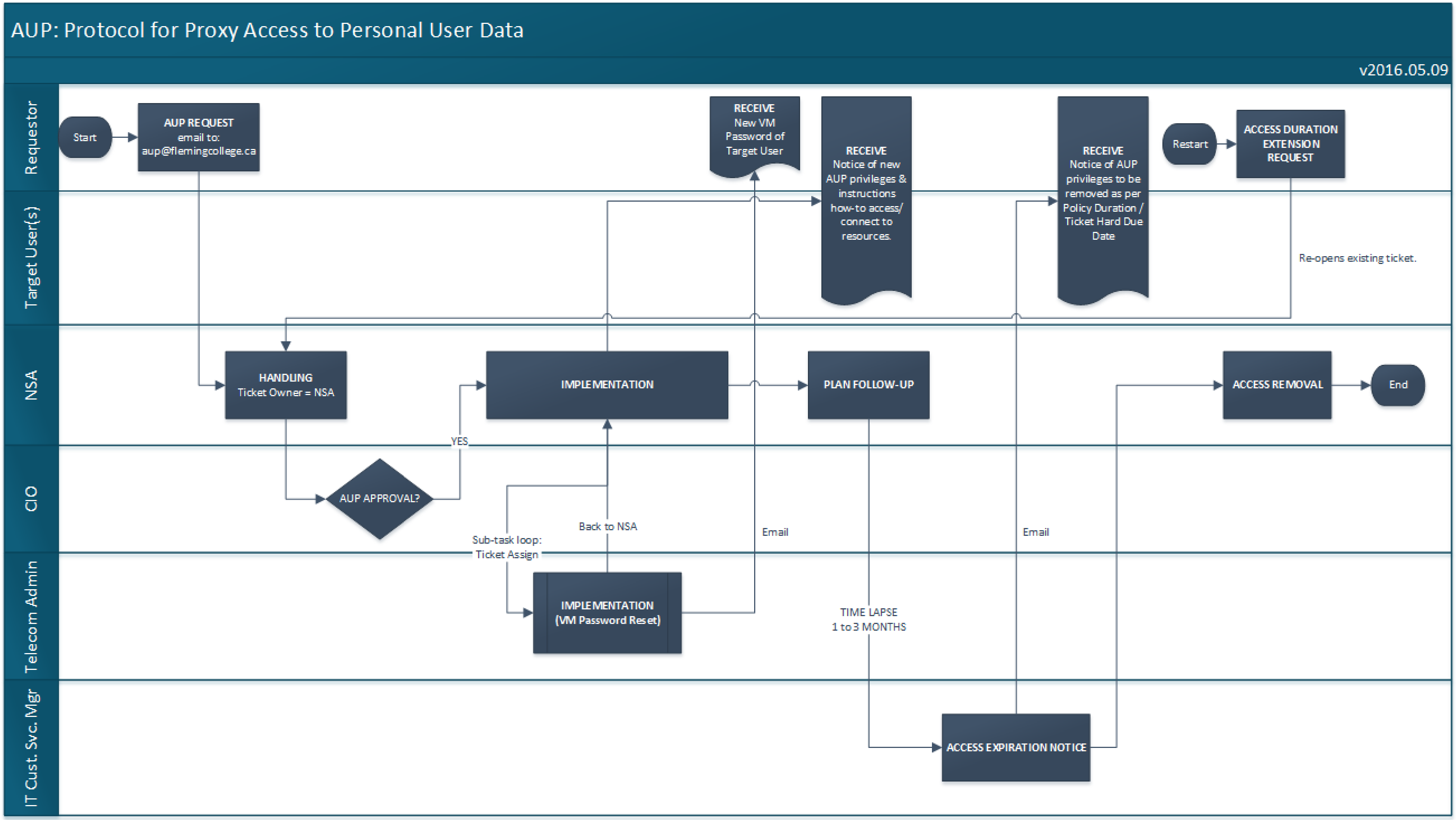
    a. The IT Customer Services Manager Administrator will notify the Requestor and Target User(s) via email that the AUP privileges will be removed on the Hard Due Date as per the duration specified by the AUP Policy.

    b. IT Customer Services Manager will set the Ticket Owner as the NSA once the notice has been sent.

7. Access Removal: Unless the CIO has indicated to the NSA in writing than an extension is granted, the NSA is to proceed to remove the AUP provisioned access on the Hard Due Date. The NSA will log the access removal actions via the ticket and set the ticket status to Closed.

Note: Access Duration Extension Request: During or after Access Expiration Notice or Access Removal steps (6 & 7) have occurred, the Requestor may indicate that an extension is needed and the reason why. Regardless of ticket status, the existing AUP Ticket will be re-opened & re-used for subsequent duration extension request(s). An NSA will be set as the owner of the ticket, the ticket status set to ‘open’, and the NSA is again responsible for bringing the in-queue extension request to the attention of the CIO. From there, the process above will resume at step 3.) Approval.

3.1 Swim Lane Diagram


AUP: Protocol for Proxy Access to Personal User Data
v2016.05.09
Requestor
Target User(s)
NSA
CIO
Telecom Admin
IT Cust. Svc. Mgr
Start
AUP REQUEST
email to:
aup@flemingcollege.ca
RECEIVE
New VM
Password of
Target User
RECEIVE
Notice of new
AUP privileges &
instructions
how-to access/
connect to
resources.
RECEIVE
Notice of AUP
privileges to be
removed as per
Policy Duration /
Ticket Hard Due
Date
Restart
ACCESS DURATION
EXTENSION
REQUEST
Re-opens existing ticket.
HANDLING
Ticket Owner = NSA
IMPLEMENTATION
PLAN FOLLOW-UP
ACCESS REMOVAL
End
YES
AUP APPROVAL?
Back to NSA
Sub-task loop:
Ticket Assign
Email
Email
IMPLEMENTATION
(VM Password Reset)
TIME LAPSE
1 to 3 MONTHS
ACCESS EXPIRATION NOTICE