Fleming College
LEARN | BELONG | BECOME

ADMINISTRATIVE OPERATING PROCEDURE: Remote Access

Procedure ID:	#OP 6-601A
Approved by Executive Leaders Team:	New - November 2018
Effective Date:	December 2018
Next Review Date:	2020
Monitoring Responsibility:	CIO / ITS
Linked to a College Policy:	# 6-601 *Information and Communications Technology (ICT) Appropriate Use Policy*

Policy Statement

Remote network access is provided for Fleming College employees who find themselves working from a remote location, such as home or when on-call. This access can also be provided to consultants or contractors with the sponsorship of a Fleming College Employee. While the technology used follows industry best practice, remote access is inherently a security risk and must be controlled to ensure the confidentiality, integrity and availability of College systems and information. Consequently, standards and procedures are required to minimize this risk.

This document outlines requirements that must be adhered to when using, deploying and administering remote access services to connect to Fleming College network, systems and data from an "untrusted" source (e.g. Internet, non-College device).

Definitions/Acronyms

In Scope: The granting of an exception to the usual standard remote access services that require specialist setup and circumvent the normal controls of a standard user. This includes staff and contractors requiring remote access to core systems beyond those available to a standard user via usual web services. This access can be a mix of direct access to systems using standard or privileged accounts.

Out of Scope: The use of publicly distributed material such as the website, or highly controlled environments with a customer front end such as the College web services or e.g. College owned Office 365 and the 'myCampus' portal.

Operating Procedure

Each request can be highly specialized 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 Director of IT operations or Director of Information Systems Group.

The College will operate under the following principals.

1. Authorization

a) The authorization procedure for remote access will be centrally managed by ITS.
b) College employees, consultants and contractors are eligible for remote access but are not automatically granted remote access privileges.
c) Consultant and contractor access require the sponsorship of a Fleming College Employee.
d) Remote access to resources on the Fleming College private network must be facilitated using the College Remote Access Protocol – attached.

e) Only authorized remote access mechanisms provided by ITS may be used to gain access to the Fleming College IT network.
f) All systems and services not purposely made publicly available through the internet by ITS must be accessed through the College provided remote access mechanisms.

2. ITS Requirements

a) The Remote Access Request protocol has been completed to satisfaction.
b) Remote control/desktop software, unless specified under Remote Access Mechanisms (see Appendix A), are strictly prohibited.
c) Firewalls and other technology that will be used to restrict remote access to only approved remote access mechanisms.
d) The remote access users are expected to have an existing connection to the Internet i.e. the College will not provision ISP (internet) services for remote users.
e) The remote access user may be subject to monitoring for compliance.

3. Remote Access User Responsibilities

Remote users are expected to:

a) Exercise good judgment and having awareness of key cyber security issues.
b) Avoid use of public terminals.
c) Not attempt to gain other system access or data not associated with the purpose of the remote connection.
d) Not deliberately alter data. Any changes to data will be made in such a way as to preserve the information.
e) Protect Fleming College systems and data from unauthorized individuals.
f) Report any suspected security breaches to the ITS Help Desk

4. Authentication and Accounting

a) The identity of a user connecting via a remote access service must be authenticated using College systems upon each session. Automated logins are not permitted.
b) Remote access authentications must be handled by College systems only.
c) The use of generic user names is prohibited
d) The use of generic account names is prohibited
e) The accounting system for remote access will be centrally managed by ITS. Audit logs will be maintained by ITS.

Non-compliance

Remote access may be blocked at any time as determined by the Chief Information Officer or delegate considering the following:

a) Failure to adequately protect College data or systems.
b) Evidence of security compromise in login credentials and/or hardware or software used for remote access.
c) Any violation of the Fleming College Acceptable Use Policy.
d) Blocked access may be reinstated with verification that the problem(s) that resulted in access being blocked have been adequately addressed and resolved.

College employees found in violation may be subject to disciplinary action, up to and including termination.

Exceptions and complaints

Exceptions, complaints, exemptions or questions regarding the contents, applicability and provisions of this standard must be referred to and approved by Chief Information Officer of Fleming College or delegated authority.

Related Documents

- College Policy #6-601, *Information & Communications Technology and Appropriate Use Policy*
- College Administrative Operating Procedure #OP 6-601, *AUP and Accessing Another User's Data*

Appendices

- Appendix A: *AUP Protocol for Access to College Core Systems*

History of Amendments/Reviews

Summary of Changes	Date
New procedure; developed in response to the 2018 cyber security review	• SMT Nov. 13, 2018

AUP: Protocol for Access to College Core Systems

Document Information

Document Title	AUP: Protocol for access to College core systems
Department	ITS
Owner	Roger Fitch, CIO
Author(s)	Derrick Davidson NSA
Publish Location	
Revision Date	13-May-2016
Version #	1.0
Document Status	Draft

Document History

Version	Date	Details
1.0	18 Oct 2018	Initial version. /DD

Contents

1 Objectives

This protocol is linked to College administrative operating procedure 6-601A and defines the specific actions ITS services take when granting any user access to College Core systems by a non-standard or untrusted source e.g. internet.

In Scope: This document describes the ITS protocol and controls used when granting of an exception to the usual standard remote access services that require specialist setup and circumvent the normal controls of a standard user. This includes staff and contractors requiring remote access to core systems beyond those available to a standard user via usual web services. This access can be a mix of direct access to systems using standard or privileged accounts.

Out of Scope: The use of publicly distributed material such as the website, or highly controlled environments with a customer front end such as the College web services or e.g. College owned Office 365 and the 'myCampus' portal.

2 Protocol Overview

Protocol Name:	**AUP:** Protocol for access to College core systems
Owner:	CIO, Roger Fitch
Points-of-Contact:	Director IT Operations, Paul Marchant. Director Information Systems Group, George MacDougall

Remote network access is provided for Fleming College employees who find themselves working from a remote location, such as home or when on-call. Remote access to the Fleming College network is also provided to consultants and contractors with the sponsorship of a Fleming College Employee. While the connection is as secure as possible, remote access is inherently a security risk and must be controlled to ensure the confidentiality, integrity and availability of College systems and information. Consequently, standards and procedures are required to minimize this risk. The procedures provided in this document were developed to minimize risk associated with this activity. This procedure must be followed to ensure the integrity of the College's network and to protect all users of College systems.

3 Definitions

ITS - Information Technology Services. The technology department of Fleming College.

VPN – Virtual Private Network. A secured private network connection built on top of a public network. VPN provides a secure tunnel over the internet between a computer and a private network.

NSA – Network Support Analyst. An employee of the College within the ITS department who is responsible for network operations.

CIO – Chief Information Officer.

Service Ticket – A singular email thread that exists within the ITS ticket system to help manage service requests, issues and incidents.

Ticket watcher – The NSA is actively assigned to manage ticket queues.

Approval Agent - A manager at the College within the ITS department who is accountable for network operations. Typically, the Director of Information Technology or Chief Information Officer.

Network Service – Refers to a client/server protocol that is providing access. Examples include RDP and SSH.

AD - Active Directory is a directory service that Microsoft developed for the Windows domain networks. A directory is a hierarchical structure that stores information about objects on the network.

4 Oversight

At the ITS Leaders weekly meeting (Friday mornings), the remote access request bucket within the ticket system will be reviewed with respect to:

a) New remote access requests
b) Requests pending CIO approval
c) Upcoming access expirations
d) Timely removal of access privileges

5 Process Steps

1. The following procedures should be followed to acquire remote access:

Requester will submit an ITS service ticket via email:

a) Send email To: remoterequest@flemingcollege.ca
b) Please use the Subject: “Remote Access Request”
c) An automated email response from our ticket system will provide the requestor with a Remote Access Request Form.

2. Requester must fill out and submit the Remote Access Request Form by responding to email thread.

The ticket will then be:

a) Placed into the appropriate queue (Network Services Remote Access Requests)
b) Assigned to an approval agent:
c) Evolve System Director, College Information Services
d) All other Systems Director, IT Operations

3. If approved, the ticket will then be assigned to an NSA ‘ticket watcher’.

4. If the request is denied, the approval agent will respond to the requester with adequate explanation and proceed to close the ticket.

5. The approval agent may choose to request further information of the requestor before assigning an owner to the ticket.

6. The NSA will ensure appropriate AD credentials exist or will create the AD credentials.

    a) The remote access user is to be located in an appropriate container.
    b) The password shall conform to the Fleming College password standard.
    c) The account description should note the requestor information.
    d) The expiry date shall be set according to the terms outlined in the remote access request form.
    e) The remote access user is to be assigned to the appropriate directory group(s) controlling remote access.

7. The NSA will review all associated security policies for compliance. If the network access requested is not provisioned, the NSA will provision security policies accordingly:

    a) The NSA may involve other ITS staff to provision information systems access.
    b) The ticket may be assigned to the appropriate IT staff for this provisioning.
    c) The ticket will then be re-assigned to the NSA once systems provisioning is complete.
    d) All provisioning will implement a 'least privilege' security posture (i.e. 'destination' hosts, networks or users are as specific as possible).

8. The NSA will confirm the remote connectivity to the Fleming College network and check access is limited to the "least privileged" method for the approval and the resources being requested. Once complete:

    a) The ticket will be updated with credential details and confirmation of access.
    b) The ticket will be move to the next appropriate queue (Service Desk □Inbox).

9. A Service Desk member will take ownership of the request and ensure:

    a) Instructions for connecting to the Fleming College VPN are attached to the ticket
    b) Offer their assistance if requestor is on-site (including installation of VPN client).
    c) Answer questions as they arise from requestor.
    d) Follow-up on the request as per expiry date and assigned back to the NSA.

10. The NSA will ensure:

    a) Active Directory account is expired
    b) All provisioned security policies are modified (or disabled) to remove access.
    c) This may involve follow-up with information systems contact from 6a.
    d) Ticket is updated to indicate remote access has been removed.
    e) Ticket is assigned to Manager, IT Customer Service.

11. The Manager, IT Customer Service will review (weekly) and ensure ticket closure.

Appendix A to AUP: Protocol for access to College core systems

External to Internal

Fleming College requires the use of the Global Protect VPN client from external untrusted zone connections to the Fleming College network. Subsequent systems access may be obtained using the following secure mechanisms:

- HTTPS
- SSH
- RDP
- Fleming College VDI.

Internal to External

Fleming College sanctions system access via the use of the following secure mechanisms from internal trusted zone connections to the Fleming College network:

- Cisco WebEx

VPN Client

The Global Protect client may be downloaded via this software portal: https://gp.flemingc.on.ca