


POLICY TITLE	SS-13 Remote Access
POLICY HOLDER	Student & Infrastructure Support
ORIGINAL DATE	December 2014
REVIEW DATE	April 29, 2015
REVISED DATE	April 29, 2015
NEXT REVIEW	December 2019

POLICY

The purpose of this policy is to define standards for connecting to Yukon College's network from outside of the college.

Approval Statement

With the consent of the Senior Executive Committee and approval of the President this policy is hereby deemed in effect the 29 day of April, 2015



 President, Yukon College

April 29, 2015

 Date

1.0 PURPOSE

The purpose of this policy is to define standards for connecting to Yukon College's network from outside of the college. These standards are designed to minimize the potential exposure to Yukon College from damages which may result from unauthorized use of Yukon College resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Yukon College internal systems, etc.

2.0 GOVERNING LEGISLATION AND RELEVANT DOCUMENTS

- Acceptable Use of Technology Policy
- Password Policy
- Wireless Communications Policy

3.0 SCOPE

This policy applies to all Yukon College employees, with a Yukon College owned portable device or workstation used to connect to the Yukon College network. This policy applies to remote access connections used to do work on behalf of Yukon College, including reading or sending email and viewing and/or accessing intranet/personal resources. Remote access implementations that are covered by this policy include, but are not limited to digital subscriber line (DSL), virtual private network (VPN), secure shell (SSH).

4.0 POLICY

It is the responsibility of Yukon College employees, contractors, vendors and agents with remote access privileges to Yukon College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Yukon College.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Yukon College's network:

- Wireless Communications Policy

- Acceptable Use of Technology Policy

For additional information regarding Yukon College's remote access connection options, including how to order or disconnect service, troubleshooting, etc., please contact IT Services.

5.0 REQUIREMENTS

- 5.1.1 Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *Password Policy*.
- 5.1.2 At no time should any Yukon College employee provide their login or email password to anyone, not even family members.
- 5.1.3 Yukon College employees and contractors with remote access privileges must ensure that their remotely connected Yukon College-owned computer or workstation is not concurrently connected to any other network.
- 5.1.4 Yukon College employees and contractors with remote access privileges to Yukon College 's corporate network must not use non- Yukon College email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct Yukon College business, thereby ensuring that official business is never confused with personal business.
- 5.1.5 Non-standard hardware configurations must be approved by IT Services.
- 5.1.6 All hosts that are connected to Yukon College internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers (if permitted).
- 5.1.7 Use of personal equipment to connect to Yukon College network infrastructure may be approved as long as the equipment meets the College requirements for remote access. Yukon College users can access internet enabled applications (email, portal, FAST) from their personal computers as needed.

6.0 POLICY COMPLIANCE

6.1 Compliance Measurement

The IT Services team will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by IT Services in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 FORMS

N/A.

8.0 APPENDICES

N/A

9.0 ADDENDUMS

Addendum A – Policy Communication Checklist

ADDENDUM A - POLICY COMMUNICATION CHECKLIST

Policy Name: Remote Access
 Number: SS-13
 Submitted by: Colleen Wirth

List those consulted with in preparation of this policy:

Name	Department	Date
Lynda Pattie	IT consultant	April 2015
Mike Barwell	IT Services Manager	

The order for communication and/or consultation for a new or revised policy is as follows:

1. SEC – initial review and recommendations from SEC membership;
2. Identified stakeholders within Yukon College in order of priority – see below;
3. SEC – to be briefed on any issues arising out of stakeholder consultations;
4. Staff – SEC members to bring policy to their staff for feedback (*SEC member introducing this policy is responsible for sending to SEC, requesting that it be circulated to their staff for feedback*);
5. SEC – final draft supported by SEC membership and approved by the President.

This checklist must be completed prior to the final draft of a policy being presented to SEC for presidential approval.

Body	Communication Planned	Completed	Comments
SEC	December 17, 2014		
Student Union	n/a		
Employee's Union	n/a		
Occupational Health and Safety	n/a		
Academic Council	n/a		
Board or a Board subcommittee	n/a		
YC Staff	April 2015	April 2015	
<i>Other</i>			
SEC for Final Review	April 29, 2015		