Remote Access Policy – IT 13.0
Information Technology

Policy Title:	**Remote Access**
Policy Approver:	President’s Office
Policy Holder:	IT Director
Category:	Operational
Original Date:	December 2014
Last Revised:	April 2015
Next Review:	December 2019

Policy Statement

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

Approval Statement

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

Karen Barnes

President, Yukon College

April 29, 2015

Date

1. Purpose of Policy

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

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

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

- Wireless Communications Policy
- Acceptable Use of Technology Policy

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

2. Governing Legislation and Relevant Documents

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

3. Scope

This policy applies to all Yukon University employees, with a Yukon University owned portable device or workstation used to connect to the Yukon University network. This policy applies to remote access connections used to do work on behalf of Yukon University, 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. Requirements

4.1 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.

4.2 At no time should any Yukon University employee provide their login or email password to anyone, not even family members.

4.3 Yukon University employees and contractors with remote access privileges must ensure that their remotely connected Yukon University-owned computer or workstation is not concurrently connected to any other network.

4.4 Yukon University employees and contractors with remote access privileges to Yukon University 's corporate network must not use non- Yukon University email accounts (i.e., Hotmail, Yahoo, Gmail), or other external resources to conduct Yukon University business, thereby ensuring that official business is never confused with personal business.

4.5 Non-standard hardware configurations must be approved by IT Services.

4.6 All hosts that are connected to Yukon University internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers (if permitted).

4.7 Use of personal equipment to connect to Yukon University network infrastructure may be approved as long as the equipment meets the University requirements for remote access. Yukon University users can access internet enabled applications (email, portal, FAST) from their personal computers as needed.

5. Policy Compliance

5.1 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.

5.2 Exceptions

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

5.3 Non-Compliance

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

6. Other Related and/or Accompanying Documents

Addendum A - Policy Communication Checklist

ADDENDUM A - Policy Communication Checklist

Policy Name: Remote Access
Number: SS 13.0
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 University 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	
Other			
SEC for Final Review	April 29, 2015		